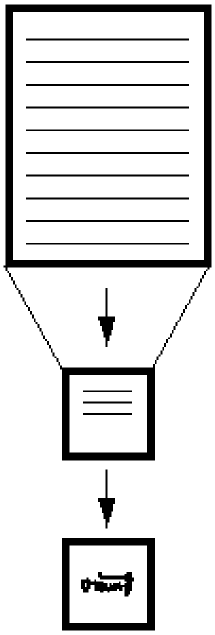
Anwendungsbericht 11

Zentrum für Paralleles Rechnen

debis Systemhaus



Kryptographische Hashfunktionen sind eine der wesentlichen Methoden der modernen Datensicherheitstechnik. Mit diesen Funktionen werden zum Beispiel sogenannte "Fingerabdrücke" elektronischer Dokumente effizient berechnet, die dann elektronisch unterschrieben werden. Damit sind die technischen Voraussetzungen für die verbindliche Übertragung elektronischer Nachrichten geschaffen, die grundlegend für die kommende digitale Revolution (elektronische Geldbörsen, Video on Demand, Teleshopping, Information Highway, usw.) sind. Gute kryptographische Hashfunktionen müssen sicher sein: So darf es z.B. keine praktische Möglichkeit geben, zwei verschiedene Nachrichten mit demselben Fingerabdruck zu konstruieren. Notwendigerweise müssen kryptographische Hashfunktionen dazu eine Reihe von statistischen Tests passieren.

Problembeschreibung

Die debis Systemhaus bat den Lehrstuhl von Prof. Schrader am Institut für Informatik der Universität zu Köln um Unterstützung bei der Entwicklung eines Programmpakets für statistische Tests kryptographischer Hashfunktionen.

Dazu wurden von den Mitarbeitern und Studenten des Instituts zunächst Vorschläge aus der Literatur klassifiziert, die Theorie dieser Tests untersucht und (nach Absprache mit der debis Systemhaus) geeignete Verfahren zur Implementierungsreife weiterentwickelt. Anschließend konnten die Tests mit einer einheitlichen Benutzeroberfläche in kurzer Zeit realisiert werden. Dabei wurde besonders auf die Portabilität und Wiederverwendbarkeit der Software geachtet.

Algorithmen

Zur Untersuchung der Auswirkung von Änderungen in der Eingabe auf die Ausgabe wurden zunächst klassische Standardverfahren wie der Lawinentest, der Abhängigkeitstest und der Korrelationstetst realisiert. Damit läßt sich z.B. ermitteln, ob einzelne Stellen der Ausgabe der Funktion von Veränderungen der Eingabe nicht berührt werden.

Die beiden Schwerpunkte des Programmpakets liegen in neuartigen algebraischen Zykeltests und der effizienten Suche nach Linear- und Pseudolinearfaktoren.

Mit den implementierten Zykeltests können für eine Funktion mit identischem Definitions- und Wertebereich Eigenschaften wie Abgeschlossenheit, Injektivität und Fixpunktfreiheit entschieden werden. Darüberhinaus kann beurteilt werden, ob das von der Größe der Schlüsselmenge suggerierte Sicherheitsmaß realistisch ist oder nicht.

Zentrum für Paralleles Rechnen — Arbeitsgruppe Prof. Dr. R. Schrader
Telefon: (0221) 470–5312
Hausanschrift: Weyertal 80, D-50931 Köln — Telefax: (0221) 470–5317
Postanschrift: ZPR, Universität zu Köln, Albertus-Magnus-Platz, D-50923 Köln — Email: zpr@zpr.uni-koeln.de

Ziel der in der Literatur zuvor nur wenig dokumentierten Linear- und Pseudolinearfaktortests ist die Suche nach (pseudo-)linearen Abhängigkeiten innerhalb der Ausgabestellen bei gleichzeitiger Änderung einer bestimmten Menge von Eingabestellen. Dazu wurden neue Verfahren zur Bestimmung von Linear- und Pseudolinearfaktoren entwickelt und implementiert, die u.a. alle Pseudolinearfaktoren mit einer Wahrscheinlichkeit oberhalb einer vorgegebenen Schranke bestimmen.

Erster Einsatz des Programmpakets

Das Institut wurde von der debis Systemhaus zudem mit der Durchführung der im Testpaket enthaltenen Tests für eine konkrete kryptographische Hashfunktion betraut.

Das Testpaket ermöglichte eine effiziente Durchführung dieser Tests. Zu einer vollständigen Beurteilung der Qualität der kryptographischen Hashfunktion müssen die Ergebnisse im allgemeinen um eine manuelle Analyse der Funktion erweitert werden.

Ansprechpartner

Dipl.–Math. Georg Wambach
Zentrum für Paralleles Rechnen
Institut für Informatik
Universität zu Köln
Pohligstr. 1
50969 Köln
Tel: 0221/470-5308
Fax: 0221/470-5317
E-Mail: gw@informatik.uni-koeln.de

Dr. Frank Damm

debis Systemhaus
IT-Sicherheit
Oxfordstr. 12-16
53111 Bonn
Tel: 0228/9841-147
Fax: 0228/9841-60
E-Mail: fd@itsec.bonn.cap-debis.de

Köln, 21. Februar 1995