Zeitschrift: Schweizer Ingenieur und Architekt
Herausgeber: Verlags-AG der akademischen technischen Vereine
Band: 111 (1993)
Heft: 19

Sonstiges

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 01.04.2025

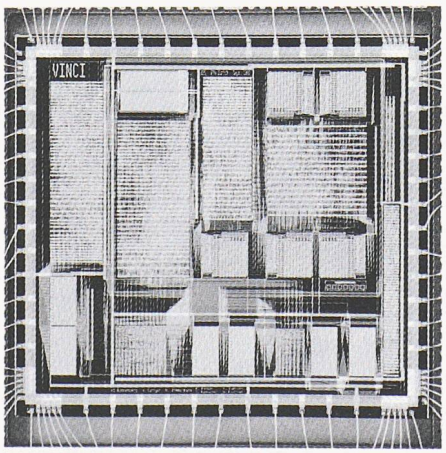
ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Aktuell

ETH Zürich entwickelte schnellsten und sichersten Kryptographie-Baustein der Welt

(pd) Wichtige Nachrichten wurden früher – beispielsweise in Kriegszeiten – von Spezialisten so umgewandelt oder verschlüsselt, dass sie nur von ihrem rechtmässigen Empfänger gelesen werden konnten. Auch die moderne Kommunikationstechnik muss dafür sorgen, dass z.B. die an einen bestimmten Telefonbenützer gerichtete Nachricht nur von ihm gehört werden kann. Auch Computerdaten, wie sie z.B. in Bankgeschäften täglich übermittelt werden, müssen geschützt werden. Wenn man bedenkt, dass heute auf einem Glasfaserkabel in einem grossen ununterbrochenen Informationsfluss gleichzeitig bis zu 30 000 Telefongespräche übertragen werden, so zeigt sich, dass dem Verschlüsseln (oder Chiffrieren) beim Absender und dem Entschlüsseln (oder Dechiffrieren) beim Empfänger eine besonders hohe Bedeutung zukommt. Die Kryptographie von einst lebt also auch in den modernsten Fernsprechsystemen von heute weiter.

Am Institut für Integrierte Systeme der ETH Zürich wurde im Rahmen eines gemeinsamen Forschungsprojekts mit dem Institut für Signal- und Informationsverarbeitung und mit der Unterstützung der Ascom Tech AG., Solothurn, sowie des Bundes ein hochintegrierter Schaltkreis mit dem Namen Vinci, ein Chip von 9,9x11 mm Kantenlänge, entworfen, welcher als schnellster und zugleich sicherster Kryptographiebaustein der Welt gilt. Die Leistungen dieses Chips sind phänomenal: Er kann pro Sekunde bis zu 5000 Seiten Schreibmaschinentext, bis zu 6000 Telefongespräche gleichzeitig oder bewegte Fernsehbilder samt Ton ver- oder entschlüsseln. Dies tut er bei einer Arbeitsfrequenz von 25 Megahertz und einer Ver- oder Entschlüsselungsrate von 178 Mio. Bit pro Sekunde.



Der nur 9,9x11 mm messende Chip Vinci, konstruiert von Forschern der ETH Zürich, ist einer der schnellsten und sichersten Kryptographie-Bausteine der Welt

Das mathematisch sehr anspruchsvolle neue Verschlüsselungsverfahren, nach welchem der Chip funktioniert, heisst IDEA (International Data Encryption Algorithm) und wurde in mehrjähriger Arbeit von Forschern des ETH-Instituts für Signal- und Informationsverarbeitung entwickelt. Es hat bisher weltweit allen Versuchen von Wissenschaftern widerstanden, welche den Verschlüsselungscode zu knacken versuchten.

251 000 Transistoren auf einem cm²

Die ausserordentlich hohe Verarbeitungsleistung auf einem einzelnen Baustein deutet auf höchste Komplexität hin. So enthält Vinci auf seiner Fläche von 108 mm² rund 251 000 Transistoren. Er dürfte damit der grösste anwendungsspezifische elektronische Baustein (ASIC) sein, der bisher in der Schweiz entworfen wurde. Seine Herstellung musste allerdings im Ausland geschehen, da die hierfür notwendigen Einrichtungen in der Schweiz nicht vorhanden sind.

Die Prüfung, ob ein solcher Baustein richtig funktioniert, gestaltet sich sehr schwierig. Aus diesem Grund haben die Wissenschafter der ETH Zürich dem Chip eine Selbsttesteinrichtung eingepflanzt, welche innerhalb von 160 Millionstel Sekunden ohne äussere Einwirkung eine Aussage über dessen Funktionsfähigkeit gestattet. Ausserdem stellt Vinci während des Ver- und Entschlüsselungsvorganges allfällige Funktionsfehler fest und rapportiert diese umgehend nach aussen.

Der Chip wurde im Hinblick auf die weltweit rasant wachsenden Bedürfnisse in der elektronischen Kommunikation gebaut. Vinci kann überall dort eingesetzt werden, wo hohe Übertragungsraten von Daten nötig sind, wie sie z.B. im Bankenbereich von Filiale zum Hauptsitz, von einzelnen Bankomaten, von automatischen Kassierstationen bei Tankstellen zum zentralen Computer, vom Börsenplatz zum Wertschriftenhändler, in der telefonischen Kommunikation oder auch im E-Mail oder im Fax-Verkehr verlangt sind. Der weltweit grosse und immer weiter wachsende Bedarf an solchen Einrichtungen dürfte Vinci auch zu einem wirtschaftlichen Erfolg machen.

Integris – das integrierte Ingenieursystem

(PSI) Mit der zunehmenden Anwendung von Computern in Architekturbüros und bei grossen Bauherren (Industrie, öffentliche Hand) gelangt die Heizungs-, Lüftungs- und Klima-Branche zunehmend unter Druck, ebenfalls Informatikhilfsmittel und effizientere Planungswerkzeuge einzusetzen. Wachsende Anforderungen (Energiesparen, behördliche Vorschriften usw.) erfordern exaktere und damit aufwendigere Planungsarbeit.

Das Paul-Scherrer-Institut, PSI, verfügt über Know-how sowohl auf dem energierelevanten Gebiet der Haustechnik als auch in der Informatik. In diesem Umfeld entstand 1987 der Gedanke, für die Planungsfirmen der Haustechnikbranche ein integriertes Softwarewerkzeug zu entwickeln. Auf der Basis eines partnerschaftlichen Finanzierungsmodells stellten Bund und Privatwirtschaft die nötigen Ressourcen für die Entwicklung des Systems zur Verfügung. Seit Beginn der Projektarbeiten im April 1987 und bis Ende 1992 wurden insgesamt rund 25 Mannjahre für das Projekt aufgewendet.

Das Resultat dieses umfangreichen Technologietransferprojektes wurde erstmals an der Computermesse «CeBit 93» in Hannover einer breiteren Öffentlichkeit vorgestellt: «Integris» ist einerseits eine leistungsfähige Entwicklungsumgebung mit eigenen Entwicklungswerkzeugen für die flexible Implementation praxisgerechter Programme für die Haustechnikplanung. Andererseits bildet Integris das Kernsystem, in das diese Programme integriert werden.

In Zukunft formuliert der Markt die Ansprüche an das System. Integris ist für einen Ausbau auf weitere Bereiche der Haustechnik (Gas-, Druckluft-, Sprinkler-, Elektroanlagen usw.) geeignet. Einsatzmöglichkeiten mit vergleichbaren Anforderungen an die Informatik finden sich aber z.B. auch in der Elektronikindustrie und in der Verfahrenstechnik.

Integris wird Anfang 1994 an alle interessierten Firmen im Bereich Software-Entwicklung und -Vermarktung gegen einen geringen Unkostenbeitrag abgegeben. Auskünfte bei: PSI, Labor für Energie- und Verfahrenstechnik, Projektteam Integris, c/o Byron Informatik AG, Riehenstrasse 60, 4058 Basel, Telefon 061 681 22 11.

Beschäftigung 1992: Alle Branchen von der Krise betroffen

(BFS) Gemäss der vom Bundesamt für Statistik durchgeführen vierteljährlichen Beschäftigungsstatistik wurden 1992 in Industrie, Gewerbe, Bau und Dienstleistungen beinahe 115 000 Vollzeitstellen abgebaut. Der Beschäftigungsrückgang betrug 4,1% gegenüber dem Vorjahr. Im Vergleich zum Jahr 1991 war 1992 dadurch gekennzeichnet, dass der Beschäftigungsabbau sich auf alle Wirtschaftsbranchen, Dienstleistungsektor inbegriffen, ausdehnte und sämtliche Regionen des Landes betraf.

Selbst wenn die Bekleidungsindustrie mit 13,3% Beschäftigungsrückgang im Jahre 1992 anteilsmässig am stärksten betroffen war, sind es die in den wichtigsten Industriezweigen festgestellten Verluste, die am meisten ins Gewicht fallen: Die Maschinen- und Fahrzeugindustrie hat rund 14 000 Stellen (–9,6%) abgebaut. Die Elektro-, Elektronikindustrie (–6700 Beschäftigte, –6%), die Holzindustrie (–5800, –9,5%), die Metallindustrie (–4900, –5,3%) und die grafische Industrie (–4600, –8,5%) sind die weiteren bedeutenden Bereiche, die zum jährlichen Nettoverlust von 50 000 Beschäftigten in Industrie und Gewerbe beigetragen haben (–6,6%).

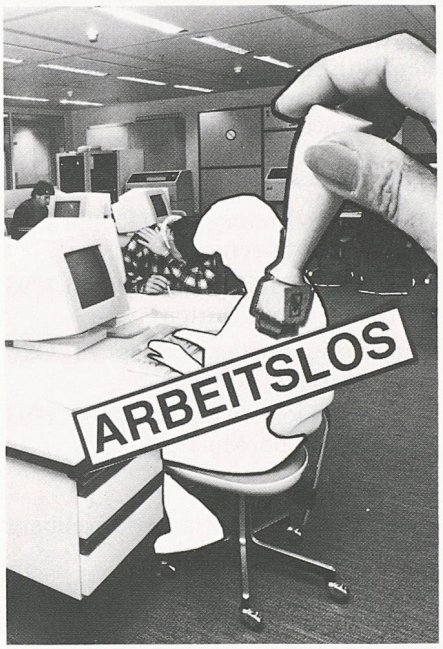
Mit Ausnahme der Kantone Wallis (–2,0%) und Freiburg (–3,0%) haben die Westschweizer Kantone 1992 höhere Beschäftigungsverluste zu verzeichnen als im schweizerischen Durchschnitt. Genf (–7,8%) und Waadt (–6,1%) sind die am stärksten betroffenen Kantone. Aber auch die anderen grossen Kantone wurden von der Krise nicht verschont. Die meisten von ihnen verzeichneten Ergebnisse von rund –4,0%: Zürich (–3,8%), Bern (–4,0%), Aargau (–3,7%), Basel-Stadt (–4,0%), Basel-Landschaft (–4,1%).

Dienstleistungssektor: 62 000 Stellen abgebaut

Der Beschäftigungsabbau im Dienstleistungssektor stellt die markanteste Entwicklung im Jahre 1992 dar: Man hatte sich in den achtziger Jahren daran gewöhnt, dass der Dienstleistungssektor (beinahe 2 von 3 Beschäftigten sind in diesem Sektor tätig) die Stagnation und später den Beschäftigungsrückgang im sekundären Sektor kompensiert. 1992 wurden aber auch hier 62 000 Stellen abgebaut (12 000 mehr als im 2. Sektor). Die Folgen dieser Trendwende: Die Gesamtbeschäftigung sinkt stark und die Arbeitslosigkeit setzt jetzt auch in Berufen und Branchen ein, die bis heute wenig betroffen waren.

Allein die Beratungs- und Planungsbranche, die u.a. die Architektur- und Ingenieurbüros enthält, hat die Beschäftigung um beinahe 11 000 (–6,4%) Stellen reduziert. Das Gastgewerbe hat 7700 Beschäftigte (–4,3%), der Detailhandel 7600 (–3,1%) und das Gesundheitswesen 6400 (–4,4%) abgebaut.

Die Zunahme der Beschäftigung im Bauhauptgewerbe ist sicher eine Folge des geänderten Saisonprofils. Gemäss der Erhebung des Schweiz. Baumeisterverbandes (SBV) scheint – aufgrund verschiedener Gründe bei der Zusammensetzung der Arbeitsbewilligungen für Ausländer, den Spezialbewilligungen für Saisonniers aus Konfliktregionen und der bevorzugten Einstellung von Schweizern – der winterliche Beschäftigungsrückgang nicht so gross ausgefallen zu sein wie bis anhin.



1992 wurden in der Schweiz rund 115 000 Vollzeitstellen abgebaut. Dieser Beschäftigungsrückgang betraf alle Wirtschaftsbranchen, am markantesten aber den Dienstleistungssektor, wo 62 000 Stellen verlorengingen (Bild: Comet)

Korrigenda

Über den im Rahmen des DIANE-Projektes «Tageslichtnutzung» eröffneten Modellraum in Zürich-Oerlikon, der Architekten und Planern die Möglichkeit gibt, sich über die Vorteile der Tageslichtnutzung zu informieren, haben wir in SI+A Nr. 13 vom 25. März auf Seite 233 kurz berichtet. Leider stimmte die Telefonnummer, bei der sich Interessierte zu den Informationsveranstaltungen – die nächste findet am 27. Mai statt – anmelden können, nicht. Sie lautet richtig: 01/385 27 81.

Ganz kurz

Informatik/Kommunikation

(PTT) Die **Nachfrage nach VSAT-Diensten** (Very Small Aperture Terminals), die im wesentlichen die Datenkommunikation via Satelliten unter Verwendung von Kleinstbodenstationen umfassen, nimmt ständig zu. Vor allem grosse und mittlere Firmen mit grossen Filialnetzen bedienen sich vermehrt der VSAT-Dienste. Typische Anwendungen sind Datenverteilnetze für Finanz- und Nachrichtenagenturen, interaktive Netze für Reservationssysteme, Kreditkartenüberprüfungen, Inventurkontrollen oder die Verbindung von lokalen Netzwerken.

(PTT) Im November 1996 wird die **Zusammenlegung der PTT-Telecom-Netzgruppen** und die damit verbundene Umnumerierung abgeschlossen sein. Dannzumal werden von einstmals 51 Netzgruppen nur noch 18 bleiben, je eine pro Fernmeldedirektion und zwei für Zürich. Mit der Zusammenlegung der Netzgruppen erhalten rund 2,5 Mio. Teilnehmer neue, einheitlich siebenstellige Rufnummern.

(PTT) Im Vergleich zu 1990 wird das **prognostizierte Telekommunikationspotential in Europa** bis 1995 um nahezu 50% und bis 2010 sogar um das Dreifache ansteigen. Die Investitionen in diesem Bereich dürften – nach Ansicht des Chefs der Deutschen Telekom, Ricke – sogar um das Vierfache zunehmen. Bis zur Jahrtausendwende werde der Anteil der Telekommunikation am Bruttosozialprodukt der EG von zurzeit 3 auf 7% steigen.

(pd) Der **Berner Telekommunikationskonzern Ascom** will den Bereich Teilnehmervermittlungsanlagen (TVA) in Solothurn zusammenlegen (bisher an den Standorten Bern und Solothurn) und baut deshalb 100 bis 200 Stellen ab. Die zunehmende Globalisierung der TVA-Märkte und der damit verbundene Konkurrenz- und Preisdruck zwinge zu dieser einschneidenden Massnahme.

(FhG) Das Fraunhofer-Institut für Graphische Datenverarbeitung in Darmstadt hat in Zusammenarbeit mit dem Zentrum für Graphische Datenverarbeitung einen **Arbeitskreis zu Themen der Virtuellen Realität gegründet.** Ziel ist es, ein Forum für einen freizügigen Informations- und Erfahrungsaustausch sowie für Grundsatzdiskussionen zur VR bereitzustellen.