Computer and Communications

Security Reviews

Volume 3 Number 4 (December 1994) ISSN 1352-6278

CONTENTS

This journal reviews research in computer and communications security. Work published in major journals and conferences is covered automatically; local publications (such as research reports) should be sent to the editor, care of the University Computer Laboratory, Pembroke Street, Cambridge CB2 3QG, United Kingdom.

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by 31 November 1994; and most books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

IEEE Infocom 94: Thirteenth Annual Joint Conference of the IEEE Computer and Communications Societies, 14–16 June 1994, Toronto, Canada; *proceedings published by the IEEE*

Compass 94: Ninth Annual Conference on Computer Assurance, 27 June – 1 July 1994, National Institute of Standards and Technology; *proceedings published by the IEEE*

PDC 94: Thirteenth Annual ACM Symposium on Principles of Distributed Computing, 14–17 August 1994, Los Angeles, California; *proceedings published by the ACM*

Crypto 94: 22–25 August 1994 at Santa Barbara, California, USA; *proceedings published by Springer as LNCS v 839*

PDIS 94: Third International Conference on Parallel and Distributed Information Systems, 28–30 September 1994, Austin, Texas

EDCC-1: 4–6 October, Berlin, Germany; *proceedings published by Springer as LNCS v 852*

NCSC 94: Seventeenth National Computer Security Conference, 11–14 October, Baltimore, Maryland; *proceedings published by the National Institute of Standards and Technology*

ESORICS 94: Third European Symposium on Research in Computer Security, 7–9 November, Brighton, England; *proceedings published by Springer as LNCS v 875*

Chinacrypt 94: 11–15 November 1994 at Xidian, China; *proceedings published as ISBN 7-03-004363-4/TP.398*

Owing to pressures of time and space, and the large number of conferences which are held in the last quarter of the year, we have not been able to include all the reviews from NCSC 94 and ESORICS 94, and have had to hold over the reviews of Cardis, Asiacrypt and Fairfax. These should appear in volume 4 issue 1.

We regret that copyright laws prevent us from supplying copies of articles reviewed in this journal.

1 Applications and Engineering

034101 'Molecular Computation of Solutions to Combinatorial Problems'
LM Adleman, *Science v 266 (11 Nov 94) pp 1021–1024*

The author reports solving the Hamiltonian circuit problem for a directed graph with 7 vertices using the techniques of molecular biology. Each vertex was associated with a random 20-mer sequence of DNA and each edge with sequences which contained the appropriate 10 end bases of its two terminating vertices. These chemicals were mixed, and the ligation reaction generated DNA molecules encoding random paths in the graph. Polymerase chain reactions were then used to amplify those paths with given endpoints; chromatography to isolate those paths with exactly seven vertices; and affinity purification to remove those which missed any of the vertices. The energy efficiency of this technique potentially exceeds that of electronic computers by many orders of magnitude.

034102 'Why Cryptosystems Fail'
RJ Anderson, *Communications of the ACM v 37 no 11 (Nov 94) pp 32–40*

This is an updated journal version of the author's Fairfax paper (**031103**) on the failure modes of electronic banking systems. A number of case histories of ATM fraud are discussed: the overall pattern is that most real losses are due to processing errors, or to thefts by staff or from the post, while assorted blunders in system design and operation account for almost all the rest. The conventional threat model, of a capable motivated attacker, was wrong; attacks were essentially opportunistic. Another lesson is that explicitness is fundamental to robust security. One must be explicit not just about threats, but about how these are tied to mechanisms and how the system will be operated; it is the failure to do this which causes the typical loophole.

034103 'ATMs go out-of-town'
Banking World v 12 no 11 (Nov 94) pp 28–35

The annual survey of Britain's ATM population shows that in June 1994, there were 15180 machines operated by banks and 3830 operated by building societies. There was little growth in the high street but an increasing number of machines at supermarkets, stations, airports and other out-of-town sites. Some operators are starting to sell travellers' cheques, tickets and other services through some of their machines.

034104 'Providing the X.500 Directory User with QOS Information'
P Barker, *Computer Communication Review v 24 no 3 (July 94) pp 28–37*

The author recounts the experience gained in a UK academic pilot project on the quality of service provided by X.500. Including information on which parts of the directory are most reliable turns out to be a valuable service.

034105 'Network Firewalls'
SM Bellovin, WR Cheswick, *IEEE Communications Magazine v 32 no 9 (Sep 94) pp 50–57*

The authors summarise their book on firewalls (*review section*). Firewalls may be used internally as well as at the external interface, and can implement a number of policies. There are three main types: application-level gateways, circuit-level gateways, and packet filters. A typical rule set is given for a packet filter; other provisions may need to be made for ftp and certain other services.

034106 'BFE Applicability to LAN Environments'
T Benkart, D Bitzer, *NCSC 94 pp 227–236*

Blacker front ends are the only A1 rated packet encryption devices, and so the authors tried to integrate them into a LAN. Protocol conversion and configuration issues are discussed, and performance measurements are reported for an operational internet. On the basis of these, a performance model is developed.

034107 'Secure Access to Data Over the Internet'
E Bina, R McCool, V Jones, M Winslett, *Proceedings of PDIS 94*

The authors propose a security framework for Mosaic which is designed to facilitate database access over the Internet. The mechanism is a rôle wrapper, which translates accompanying credentials of incoming queries to rôles which the database application can deal with. An example application was built using PEM.

034108 'Applying COMPUSEC to the battlefield'
DM Bishop, *NCSC 94 pp 318–326*

US army tactical systems used to be exempt from TCSEC, but this is changing as they become networked. However, applying A1 requirements to everything would be counterproductive, and a lot of commonsense is needed to decide what features are really needed - passwords may be unacceptable in combat, for example. One problem is that mission requirements and tactical compromises are not considered until well into the accreditation phase; a more sensible development methodology is suggested.

034109 'Issues and Mechanisms for Trustworthy Systems: Creating Transparent Mistrust'
M Blaze, J Lacy, T London, M Reiter, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 30–39*

The authors describe a number of AT & T developed security software products, including the cryptographic File System (which now supports organisation level key escrow), the swIPe system for IP datagram security, and the CryptoLib library of cryptographic algorithms in C. They discuss issues of trust involved in building systems from such tools.

034110 'Electronic Marking and Identification Techniques to Discourage Document Copying'
J Brassil, S Low, N Maxemchuk, L O'Garman, *IEEE Infocom 94 pp 1278–1287*

The authors describe an AT & T system to discourage illegal document copying by marking documents with line-shift encoding. Successive lines of text are shifted up or down by 1/300″, thereby encoding a serial number. Experiments on postscript documents showed that even third photocopies could be scanned and decoded with very few errors; different detection techniques are discussed, as are the effects of image defects and the countermeasures available to infringers.

034111 'High tech helps card fraud decline'
Cards International no 117 (29 Sep 94)

In the first quarter of 1994, VISA International's fraud losses dropped 18.3% to $135.9m, or 0.1% of total sales. Counterfeiting made up $37.5m of this, which was down 15.5% and is attributed to the introduction of CVVs (cryptographic checksums on card strips). Mastercard, however, saw counterfeit losses rise 67% to $37.8m, and in July ordered its member card issuers to introduce similar checksums.

034112 'Design of the Virtually Integrated Database Management System and the X.500 Directory Service for the Human Genome Project'
K Cheang, YB Choi, A Tang, *IEEE Infocom 94 pp 1293–1300*

The human genome project generates information on a number of incompatible databases scattered round the world, and the goal of its security architecture — which is based on X.500 — is to achieve a virtual integration which will allow consistent and controlled update without forcing a complete redesign.

034113 'BITS: A Smartcard Protected Operating System'
PC Clark, LJ Hoffman, *Communications of the ACM v 37 no 11 (Nov 94) pp 66–70*

The authors discuss current smartcard technology and describe a system which allows secure booting of a computer from a smartcard. The card contains both crypto keys and checksums for system executables; it provides a higher degree of antivirus protection than appears possible with software only solutions and could facilitiate greater personal mobility in computer usage.

034114 'Microsoft bids for control of home banking'
Computer Business Review v 2 no 11 (Nov 94) pp 33–34

Microsoft's $1.5bn purchase of Intuit will make it the main player in personal finance and give it control of an electronic banking operation. The business justification for the move can only be the prospect of earning fee income on transactions, and this worries banks.

034115 'Fighting cellular phone fraud'
Computer Fraud and Security Bulletin (Dec 94) pp 1–2

Cellular phone fraud has become big business in the USA since 1990, and the secret service has just arrested three men who allegedly pioneered the technique. Their modus operandi is described, as are some possible countermeasures.

034116 'Datenschutz und Kirchen'
Datenschutzberater (15 Nov 94) pp 9–10 (in German)

This article discusses the impact of German data protection law on the churches, which are among the most intensive users of personal data in that country.

034117 'Europäisches Industrie- und Forschungskonsortium entwickelt elektronisches Zahlungsverfahren'
Datenschutzberater (17 Oct 94) pp 4–7 (in German)

This article describes the CAFE project to produce a European digital cash system; it covers both the functionality and the design concepts.

034118 'Cryptographic Randomness from Air Turbulence in Disk Drives'
D Davis, R Ihaka, P Fenstermacher, *Crypto 94 pp 114–120*

It is known that the presence of a read head in a spinning disk drive causes air turbulence, both in Coriolis flow between the disk surfaces and in Taylor-Couette eddies at the rim; and that this turbulence depends sensitively on initial conditions. The authors investigated whether this could be used as a source of random bits, and found that the noise on a 1986 PC had an entropy of 100 bits per minute, with an autocorrelation which fell off within 5 seconds.

034119 'Digital Speech Compression'
J Degener, *Dr Dobbs Journal no 224 (Dec 94) pp 30–34*

The author describes the RPE-LTP algorithms used in GSM mobile telephones to compress speech to 1625 byte/sec, and provides source code for a number of tools.

034120 'Intrusion detection: approach and performance issues of the SECURENET system'
M Denault, D Gritzalis, D Karagiannis, P Spirakis, *Computers and Security v 13 no 6 (Dec 94) pp 495–508*

The authors discuss SECURENET, an experimental system funded by the EC under the RACE programme, which attempts to detect software intrusion in integrated broadband communications networks using AI techniques. Following a preliminary performance analysis, they claim that near real time detection is an attainable goal.

034121 'EDI Security'
T Dosdale, *Financial Technology Insight (Nov 94) pp 5–10*

The author describes EDI security issues and provides an overview of the options supported by EDIFACT, ANSI X.12 and ETEBAC. The cost of implementing security for such systems should by of the order of $500 for a PC and $10,000 for a mainframe.

034122 'Crime and punishment'
D Evans, *Computer Weekly (1 Dec 94) p 14*

This reports an incident in which ex-directory phone numbers were leaked by a phone company employee to a British newspaper.

034123 'Contactless Cards'
D Everett, *Smart Card News v 3 no 9 (Sep 94) pp 175–178*

The author surveys contactless smartcards, describing the engineering problems, international standards, and four typical products (all mutually incompatible). Dirty contacts are avoided, but replaced by electromagnetic noise as the main reliability issue.

034124 'Multi-application cards continued'
D Everett, *Smart Card News v 3 no 8 (Aug 94) pp 156–158*

The author discusses strategies for putting multiple applications on a single smartcard. A number of approaches are possible, but most of them use some trusted party to manage one or more master keys which then authenticate the applications.

034125 'Smart card memories'
D Everett, *Smart Card News v 3 no 10 (Oct 94) pp 194–198*

The author discusses the various memory technologies available to smart card]manufacturers, including NV–RAM, EEPROM and FRAM, and tabulates their relative performance.

034126 'Barclays: accounting for the fall in credit card fraud'
B Fergus, *Fraud Watch (Summer 94) pp 4–5*

The author describes Barclays' experience in fighting card fraud in the UK and the Far East. Better delivery, more authorisation and technical measures all contributed to a fall in fraud.

034127 'Tracing Traitors'
A Fiat, *Crypto 94 pp 257–270*

In satellite TV applications, a rogue user might leak either the key or the plaintext of an encrypted broadcast to a pirate audience; the operator will try to track such users by giving each user a personal decryption key with which he can decrypt a session key from an enabling block; thus pirate decoders can be traced. However, an attacker might take several subscriptions and try to generate an innocuous personal key from them; the author discusses various combinatorial schemes which can be used to prevent this.

034128 'BOLERO — Changing the Face of International Trade'
Financial Technology Insight (Oct 94) pp 17–18

The author describes the new Bolero system for electronic management of negotiable bills of lading and discusses its interface to the documentary credit process. Credit can be released on receipt of the shipper's digital signature on the bill.

034129 'Fund managers signing up with SWIFT want straight-through processing'
Financial Technology International Bulletin v XII no 2 (Oct 94) pp 8–9

This article describes SWIFT's success in recruiting investment management and securities firms to its network. Their transaction volumes may ultimately swamp its traditional interbank messaging business.

034130 'NatWest to participate in consumer trials of interactive home banking'
Financial Technology International Bulletin v XII no 4 (Dec 94) pp 6–8

Trials of a multimedia television service, which includes home banking and shopping, will be coordinated by BT at 2,500 homes in Colchester and Ipswich next year.

034131 'SWIFT to sue former chief executive'
Financial Technology International Bulletin v XII no 2 (Oct 94) p 3

This article describes a lawsuit by SWIFT against its former CEO, and reports a claim by the SWIFT II consultant that corners had to be cut on the project.

034132 'The ghosts of SIBOS' past return to haunt SWIFT executive committee'
Financial Technology International Bulletin v XII no 3 (Nov 94) pp 8–10

This article reports a SWIFT seminar at Boston, where member banks complained about its incursions in the securities market and the delays in setting message standards for trade confirmation and other new applications. Message robustness is also a problem, with banks spending millions to repair corrupted transactions.

034133 'Suppliers cashing in on Internet'
G Finnie, JL Schenker, *Communications Week International issue 134 (14 Nov 94) pp 36–37*

This article describes a number of firms competing to set up commercial infrastructures on top of the Internet, some of which use public key crypto.

034134 'Card sharks'
T Foremski, *Computing (20 Oct 94) p 34*

This article reports card fraud reduction techniques including a year long trial by VISA of an AI system which detects out-of-pattern transactions and which will be offered to US and European banks during 1995.

034135 'A technical approach for determining the importance of information in computerised alarm systems'
DS Fortney, JJ Lim, *NCSC 94 pp 348–357*

The authors discuss how they assessed the security of Argus, an alarm system used to protect a US nuclear weapons laboratory and which ties alarm sensors and entry controls to the security console by a network of host systems. They started from a classical site vulnerability analysis and then assessed the difference made to various attack scenarios by the alarm system, based on an explicit evaluation of all the known technical attacks on it. These included sensor defeats, equipment substitution, attacks on communications security, and tampering with the system software or configuration data.

034136 'Low tech solutions plug holes in VISA fraud prevention strategy'
Fraud Watch (Autumn 94) p 3

Forged card detection by CVVs is limited by the fact that 20% of merchants still use mechanical imprinters. VISA is now issuing card checkers to customs and law enforcement officers so that cards found on suspects can be checked.

034137 'Switch fraud control pays off'
Fraud Watch (Autumn 94) p 6

The UK debit card system Switch has kept fraud down to 0.075% of turnover — about the same as smartcard systems — by supplementing hot card files with random online checks, and by reducing floor limits of problem merchants to zero rather than by setting floor limits by sector.

034138 'Signing away crime'
Fraud Watch (Spring 94) p 5

This article reports on Kappa, a signature verification system developed at the University of Kent and tested recently at a post office near Southampton. It achieved a fraud rate of 5% and an insult rate of 2%.

034139 'Performance Aspects of the GSM Radio Subsystem'

WF Fuhrmann, V Brass, *Proceedings of the IEEE v 82 no 9 (Sep 94) pp 1449–466*

The authors describe the architecture of GSM networks, including the authentication and tracking infrastructure and the various radio channels used for access and control purposes. They provide a model of traffic intensity and call queueing, and mention some of the features of the GSM phase 2 standard, which introduces multiple encryption algorithms and better international roaming.

034140 'Statistical techniques for language recognition: an empirical study using real and simulated English'

R Ganesan, AT Sherman, *Cryptologia v XVIII no 4 (Oct 94) pp 289–331*

The authors examine what automated tests can be used to distinguish English texts from noise. The index of coincidence, χ^2 and various likelihood tests all performed well in particular circumstances. However, none of them was particularly good at distinguishing real English from a first order simulation of it.

034141 'Electronic purse a big hit in Africa'

T George, *Banking Technology v 11 no 9 (Nov 94) p 8*

This article reports on a smartcard payment system which has been fielded in Zambia and should shortly be introduced in Tanzania and Ghana too.

034142 'If you can't beat 'em, join 'em'

JA Giannone, *Cards International no 121 (1 Dec 94) pp 9 & 13*

This article discusses the technology and banking industry implications of Microsoft's link-up with VISA and its purchase of Intuit. Microsoft should get an edge in PC-based remote banking and shopping applications.

034143 'Hazards of Promiscuous Mode Programming'

W Hancock, *Network Security (Sep 94) pp 8–9*

Many LAN interfaces have a promiscuous mode for debugging purposes, and the author gives an example of how this can be turned on.

034144 'Use of Network Design to Reduce Security Risks'

L Hansen, *Network Security (Sep 94) pp 13–17*

The author describes the security features of a number of Cabletron's LAN products, which are now being extended to cope with asynchronous transfer mode.

034145 'Avis installs in-vehicle safety system'

Information Security Monitor v 9 no 11 (Oct 94) pp 1–2

Avis is fitting rental cars in Florida with a navigational and security system which uses GPS to locate the vehicle and can give detailed directions to thousands of locations. There is also a panic button to summon police.

034146 'Bills of lading go electronic'

D Jones, *Banking World v 12 no 12 (Dec 94) p 38*

Project Bolero is a scheme to replace bills of lading in Europe with electronic documents, and will be piloted in early 1995 by a number of banks and large companies. Its security is based on an online central repository operated by Mercury Communications, augmented by smartcard based encryption; it will drive both customs and banking transactions, and should be extended later to insurance certificates and letters of credit.

034147 'The listening ATM'

D Jones, *Banking World v 12 no 10 (Oct 94) p 30*

This article reports trials in Johannesburg of an ATM which uses voice recognition technology to identify customers.

034148 'Securing a Global Village and its Resources'
HM Kluepfel, *IEEE Communications Magazine v 32 no 9 (Sep 94) pp 82–89*

The author discusses the security of the SS7 telephone switching system which is widely used in the USA and elsewhere. There has been some penetration by hackers, and over 200 security bulletins have been issued by Bellcore. A number of the network security measures are described, and there is a 38-point checklist of the access control features.

034149 'Cellular Phone Fraud'
GL Kovacich, *Network Security (Aug 94) pp 7–10*

The author describes the mechanics of stealing the identity of an analogue cellular phone. This can be done using $200 worth of monitoring equipment, or even by using the maintenance mode of some phones. Eavesdropping on calls is also straightforward. Finally, a number of possible countermeasures for the mobile phone owner are discussed.

034150 'A pictorial tour of the national cryptologic museum'
L Kruh, *Cryptologia v XVIII no 4 (Oct 94) pp 381–389*

This article contains a number of photographs of exhibits at the NSA's museum at Fort Meade, Maryland, including a variety of rotor machines.

034151 'The Belgacom fall-out'
S Laurie, *Banking Technology v 11 no 8 (Oct 94) pp 34–38*

This article describes the recent upheavals at SWIFT which led to management changes, resignation of consultants, a security review and a writ against the former CEO.

034152 'What's new in the ICL world?'
A Lawes, *Computer Audit Update (Sep 94) pp 10–21*

This article reviews ICL's client-server products, including MegaServer and VME-X. The high security version of VME has been evaluated to 'UKL3' and is claimed to be 'in excess of' the 'ITSEC B1 criteria'.

034153 'The Aerospace Risk Evaluation System (ARiES): Implementation of a Quantitative Risk Analysis Methodology for Critical Systems'
CH Lavine, AM Lindell, SB Guarro, *NCSC 94 pp 431–440*

The authors describe a risk analysis tool which takes account of both preventive and mitigative controls and automates the Livermore methodology.

034154 'The Sea View Prototype: Project Summary'
TF Lunt, PK Boucher, *NCSC 94 pp 88–102*

The prototype of the Sea View MLS DBMS is based on Trusted Oracle running on Sun compartmented mode workstations; it is designed to be certifiable to class A1 when run on an A1 platform. Its design features include element-level labeling; single-level processing; a multilevel SQL; polyinstantiation integrity; and ease of evaluation. It minimises the additional trusted code by using the reference monitor of the underlying platform, and its code overhead is claimed to be imperceptible to users.

034155 'Trust in the New Information Age'
DP Maher, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 9–16*

The author describes AT & T products which sign securities transactions, prevent cloning of set-top boxes, and provide various authentication services.

034156 'Charting European Waters'
R Martin, *Cards International no 120 (10 Nov 94) pp 10–11*

In an interview, the chief executive of Europay says that edc/Maestro cards will all use PINs within 3-4 years; that $1.3bn will be invested in the next five years to bring debit cards to Eastern Europe; and that his organisation will move towards smartcards to cut the telecom costs of online authorisation.

034157 'Electronic Document Distribution'
NF Maxemchuk, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 73–80*

This article describes techniques developed by Bell labs to make it easier to identify people who redistribute electronic documents. Identifying marks can be encoded in line spacing, word spacing and font features; their relative resistance to photocopying and to various erasure strategies is discussed. Such techniques can be used, for example, to embed a purchaser's name and credit card number in a document. A trial run is scheduled for an issue of the IEEE Journal on Selected Areas in Communications in 1995.

034158 'The Disposable Telephone Card'
M Meyerstein, *Smart Card News v 3 no 11 (Nov 94) pp 214–218*

The author describes the technology of disposable chip-based telephone cards and describes the requirements envisaged by BT for their introduction into the UK. These include multiple sourcing, pan-European use and proper cryptographic protection.

034159 'Denial of Service: An Example'
RM Needham, *Communications of the ACM v 37 no 11 (Nov 94) pp 42–46*

Computerised burglar alarms are a good example of systems where the main concern is to prevent denial of service, rather than to assure confidentiality or integrity. This means detecting attacks on the network, whether by message manipulation, network flooding or simply cutting the wire. The best defences are end-to-end; if the alarm were polled by a local concentrator, then this would bring the network itself within the security envelope. An ideal system should also have anonymous communications, so that it is hard to attack the service of just one target customer.

034160 'Fighting card fraud in Germany'
J Newton, *Cards International no 120 (10 Nov 94) p 8*

This article reports a seminar on credit card fraud held in Germany in October 1994, at which a number of fraud control strategies were discussed.

034161 'Tackling payment card fraud'
J Newton, *Cards International no 119 (28 Oct 94) p 10*

The delegates at an Interpol card fraud conference in Lyons passed a motion calling for member countries to update their laws so that all forms of credit card fraud are illegal everywhere.

034162 'To catch a thief'
J Newton, *Cards International no 117 (29 Sep 94) pp 11–12*

A UK police researcher looked at the arrest of 186 people at 86 locations around the world for card counterfeiting. Most were Chinese, and 78% of the gangs had cards from the same source. His conclusion is that counterfeiting is much more organised than previously thought, and controlled by criminals with Triad links.

034163 'A Multilayer Neural network System for Computer Access Security'
MS Obaidat, DT Macchairolo, *IEEE Transactions on Systems, Man and Cybernetics v 24 no 5 (May 94) pp 806–812*

The authors describe experiments in training neural networks to recognise users by their typing patterns. With 6 users who each types 40 patterns of 15 characters, the best algorithm (back propagation) got an error rate of 2.5%.

034164 'Confidentiality and Security Concerns in the Modern Healthcare Environment'
K O'Connor, *Australian Computer Journal v 26 no 3 (Aug 94) pp 70–77*

In Australia, the Privacy Act complicates healthcare privacy by limiting the use to which personal information can be put and by giving the patient a right to access and challenge it. There are also tort law constraints, and security standards must apply to paper as well as magnetic records. A new health communications network is being developed, and this will force policymakers to tackle many of the demands for secondary use which come from epidemiologists, health insurers, debt collectors, policemen and the like.

034165 'Truly Random Numbers'
C Plumb, *Dr Dobbs Journal no 223 (Nov 94) pp 113–115*

The author discusses the random number generator in the 'Pretty Good Privacy' email encryption program for key generation. It maintains a pool of hopefully random bits, into which timing and other environmental inputs are stirred, and then distils keys from them using the MD5 hash function.

034166 'Two Russian towns get smart cards'
C Power, *Cards International no 120 (10 Nov 94) p III*

Two Russian companies have introduced smartcards to pay employees in their company towns.

034167 'Testing Intrusion Detection Systems: Design Methodologies and Results from an Early Prototype'
N Puketza, B Mukherjee, RA Olsson, K Zhang, *NCSC 94 pp 1–10*

The authors report building a testbed for intrusion detection systems. It provides a number of test scripts which simulate intrusions on multiple Unix systems by browsing, password guessing and trying to modify system files.

034168 'ASAM: A Security Certification and Accreditation Support Tool for DoD Automated Information Systems'
L Remorca, W Barr, R Zomback, VM Caputo, *NCSC 94 pp 358–369*

The authors describe the All-purpose Security Assessment Model (ASAM), a risk management tool under development by the US DoD to support certification and accreditation. In its early form, it focuses on a risk management review at the earlier stages of system development, but should be extended to the whole system lifecycle. The DoD generic threat model is discussed, as is the ASAM process flow.

034169 'Trading in tune with Bolero'
M Rowe, *Banking Technology v 11 no 8 (Oct 94) pp 48–52*

This article describes an EC-funded consortium which is developing a new EDI system for shipping documentation which will make digital signatures available for the first time in this sector and in which Cable and Wireless will act as a trusted third party; messages will be based on X.400 and EDIFACT standards. It expresses doubt about whether a single trusted third party will be adequate given the complexities of international trade.

034170 'Secure Network Access Using Multiple Applications of AT & T's Smart Card'
SA Sherman, R Skobo, RS Murray, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 61–72*

The authors describe a multi-chip, contactless smartcard developed by AT & T which supports applications from multiple vendors. Its built in operating system features include restricted file access, two way authentication, encryption and support for biometrics.

034171 'A financial management approach for selecting optimal, cost-effective safeguards for computer and information security risk management'
ST Smith, S Gale, WJ Malampy, *NCSC 94 pp 370–377*

The authors discuss combining two risk management tools — Los Alamos' LAVA and Wharton's VAM — both of which are described. The composite tool does net present value analysis of computer security investments.

034172 'The Graphical Display of A Domain Model of Information Systems Security (INFOSEC) Through Semantic Networks: A Description of the INFOSEC Semantic Network for Information Systems Security Engineers'

TT Smith, KV Dolan, *NCSC 94 pp 175–183*

The authors describe a tool developed by the NSA to facilitate the security engineer's job by organising and displaying the security relevant information about a system.

034173 'A chip off the old stripe'

S Talmor, *The Banker (Oct 94) pp 113–115*

The author discusses various initiatives to move payment card systems from magnetic strip to smartcard technology. She tabulates the card base in various developed countries, together with forecasts by GemPlus of the number of smartcards likely to be in use in Europe over the next few years. These anticipate a 30% overall growth, with even faster gains in ID cards, transportation, GSM, health and gaming.

034174 'A Confidentiality System for ISDN inter-PC High-Speed File Transfer'

K Tanaka, I Oyaizu, *IEEE Infocom 94 pp 1270–1277*

The authors describe an NTT system for encrypting files on disk and on ISDN links, using 8-round FEAL. They key setup and communications protocols are described; the latter allows an encrypted telephone conversation to be conducted at the same time as a file transfer.

034175 'Security, authenticity and integrity of electronic bills transfer based on digital signatures'

ZH Tang, *Chinacrypt 94 pp 292–297 (in Chinese)*

Based on the characteristics and security requirements of Electronic Bills Transfer, the author suggests a 3-level logical network model of funds clearing and a public key signature method. He also describes a set of regulations to suit his model, and analyses the security, authenticity and integrity of the system as well as the feasibility of arbitration.

034176 'Virtual identification is almost here'

G Torbet, *Scottish Banker (Nov 94) pp 8–9*

The author discusses possible use of biometrics in credit and debit card transactions. Third party evaluation of security claims is lacking, and the cost of devices should fall to £150 for the technology to take off.

034177 'Who are you?'

G Torbet, *Banking Technology v 11 no 9 (Nov 94) pp 46–50*

This is a survey of the possible applications of biometrics to banking. It also tabulates the fraud and error rates of the currently available technologies.

034178 'Security requirements for customer network management in telecommunications'

V Varadharajan, *NCSC 94 pp 327–338*

The author considers the security requirements of Customer Network Management, an emerging CCITT standard which gives customers online access to telecomms facilities. Typical services include online ordering of services and accounting information. Serious risks include unauthorised access and masquerading, and strong authentication is advisable.

034179 'To Serve and Protect: Reconciling Information Protection with LAN Environments'

KP Weiss, *Information Management and Computer Security v 2 no 3 (94) pp 19–25*

The author describes how a password generator from Security Dynamics can be integrated with a key management system for file encryption on LANs.

034180 'Switch - there is now a word for it, says Tim Green'

D White, *Banking World v 12 no 11 (Nov 94) pp 25–26*

This article gives the history of Britain's 'Switch' debit card system, and the reasons for the various design decisions taken. Security is essentially based on having a hot card file in every terminal.

034181 'Practical experience on EDI security'

J Williamson, *Information Security Monitor v 9 no 12 (Nov 94) pp 5–8*

The author describes some of the security concerns of the Tradanet EDI service which currently has over 5800 members. Its fault history includes wrongly notified telephone numbers causing denial of service, and software bugs or corruption leading to orders being delivered to the wrong company. Availability is the main worry though, and incorporating real network diversity is much harder than it seems. Eavesdropping is not seen as a threat: there is no record of it.

034182 'An implementation of the GSM general data encryption algorithm A5'

SB Xu, DK He, XM Wang, *Chinacrypt 94 pp 287–291 (in Chinese)*

This paper describes the data encryption algorithm A5 which is used in GSM mobile communications, and presents an implementation on a TMS320C25 digital signal processor. Experimental results of the implementation are presented.

034183 'Pretty Good Privacy'

BP Zajac, *Computer Fraud and Security Bulletin (Sep 94) pp 14–17*

The author discusses the PGP email encryption product and describes in layman's terms how it works. He also mentions some of the controversy surrounding it.

2 Operating System and Database Security

034201 'Discretionary access control by means of usage conditions'
E Born, H Stiegler, *Computers and Security v 13 no 5 (Oct 94) pp 437–450*

The authors present an access model in which objects have 'usage conditions' which are objects in their own right but in effect act as access control lists of rôles and which embody all the access information required for a particular task or method.

034202 'Decomposition of multilevel objects in an object-oriented database'
N Boulahia-Cuppens, F Cuppens, A Gabillon, K Yazdanian, *ESORICS 94 pp 375–403*

This paper proposes an approach for assigning classification labels in object-oriented systems. The model assumes the database schema to be visible (and the same) at every level, but each element of attribute value in an object can have a different classification, i.e., objects can be multilevel. Such objects are mapped into multiple single-level objects, one for each level. Objects at a given level contain the attribute values at that level plus a pointer to the objects where lower level attribute vales are stored. Execution of read, update, and write operations in this model is discussed.

034203 'Virtual View Model to Design a Secure Object-Oriented Database'
N Boulahia-Cuppens, F Cuppens, A Gabillon, K Yazdanian, *NCSC 94 pp 66–76*

The authors present a database design in which a virtual single level system is implemented on top of a multilevel object store. They describe transaction flow, implementation, and how multilevel objects are managed. The commit procedure needs to be nonstandard, and a virtual database extractor must also be provided; otherwise standard products can be used.

034204 'Mark-and-sweep garbage collection in multilevel secure object-oriented database systems'
A Ciampichetti, E Bertino, L Mancini, *ESORICS 94 pp 359–373*

This paper proposes an approach for garbage collection in object-oriented systems where objects are assigned security classifications. The approach is based on a set of untrusted collectors, one at each security level, controlled by a trusted collector. The garbage collection technique employed is mark-and-sweep, and is activated when a message flow arises. Each collector marks all objects reachable at that level, and creates a copy of any unmarked object it finds at a lower level. After all untrusted marking operations, the trusted collector removes all unmarked objects.

034205 'Information flow controls vs inference controls: an integrated approach'
F Cuppens, G Trouessin, *ESORICS 94 pp 447–468*

This paper discusses the problem of controlling unauthorized disclosure of information through internal information flow or inference. The former is concerned with the leakage of sensitive information through indirect access, while the latter deals with leakage through observation of low level related information. The method is based on the definition, for each subject, of the information the subject is explicitly permitted access and of the information the subject is explicitly denied access. Internal flow controls are enforced via causality, by ensuring that the information a user can observe depends only on information the user is permitted to know. Inference controls are enforced via policy consistency, i.e., a user cannot be both permitted and forbidden (either directly or indirectly) access to some information.

034206 'Making secure dependencies over a LAN architecture for security needs'
B d'Ausbourg, *NCSC 94 pp 114–122*

The author describes an experiment to eliminate covert channels in a LAN based system by building an access control protocol - a multilevel version of CSMA/CD -

into the LAN's hardware interface units. The system can interface with a multilevel machine such as the author's M^2S which can be used to share data between levels, and either confidentiality of integrity can be supported in multilevel mode.

034207 'Architectures for C2 DOS/Windows - based Personal Computers'
J Epstein, G Grossman, F Maxwell, N Veirs, A Donaldson, C Haley, *NCSC 94 pp 264–273*

The authors give a detailed discussion of the problems with enhancing DOS and Windows systems to C2. Although there are security front ends which provide the appearance of C2 features, the lack of memory protection means that their strength depends on the obscurity of their implementation; although 80x86 chips can provide virtual 8086's in protected mode, they cannot provide virtual 80386's. One approach might be to put the TCB in a separate CPU, such as in the disk controller, although this has never been done in an evaluated system. Protecting volumes instead of files would be easier, but would fail to meet audit requirements.

034208 'Designing Secure and Reliable Applications using Fragmentation - Redundancy - Scattering: an Object-Oriented Approach'
JC Fabre, Y Deswarte, B Randell, *EDCC-1 pp 21–28*

The authors develop their concepts of fragmented processing for object based models of computation, so that the fragments can contain code as well as data. The object approach helps solve problems such as how to deal with global variables which had been problematic for previous fragmented processing systems. They discuss confidentiality constraints, the design process and the algorithms for redundancy and scattering.

034209 'Towards a privacy-friendly design and use of IT-security mechanisms'
S Fischer-Hubner, *NCSC 94 pp 142–152*

Traditional IT security methods are not optimal for protecting the privacy of personal data, and may even endanger it. Authentication mechanisms may reveal the user's presence to third parties; access control mechanisms may reveal the user's status; while audit and monitoring systems may reveal her behaviour. An alternative security policy is presented: its goals are to ensure that data processing is necessary, and to control the purposes for which personal data are used; and its mechanisms enforce need-to-know and data subject consent. Environmental factors such as the use of pseudonyms are also important.

034210 'Artificial Intelligence and Intrusion detection: Current and Future Directions'
J Frank, *NCSC 94 pp 22–33*

Most intrusion detection systems up till now have been hand built, and the author examined whether feature selection techniques from AI could be used in future to home in automatically on the most useful indicators. His goal was to analyse SMTP connections to discover whether any rogue private networks had been set up, and his experimental results are presented.

034211 'Does Licensing Require New Access Control Technologies?'
RC Hauser, *Communications of the ACM v 37 no 11 (Nov 94) pp 48–55*

Software licensing schemes can work by metering usage or by restricting the maximum number of permitted users. Enforcing the latter type can be tricky, as neither mandatory nor discretionary access control models support it, and current solutions depend on the obscurity of features in the application code. A proper solution should protect not just executable code, but also databases, encyclopaedias and the like; it is suggested that an extra permission bit be added to show when a file is subject to licensing, so that the file server can consult a licence server before releasing it. Various engineering tradeoffs are discussed.

034212 ‘CMW Introduction’

G Huber, *ACM SIGSAC v 12 no 4 (Oct 94) pp 6–10*

The author discusses the US DoD’s compartmented mode workstation programme, and mentions the five current vendors. He describes the mechanics of trusted windowing; although developed for the intelligence community, it has proved applicable in operations, logistics and drug enforcement too.

034213 ‘Independent Validation and Verification of Automated Information Systems in the Department of Energy’

WJ Hunteman, R Caldwell, *NCSC 94 pp 468–477*

The authors describe the US department of energy’s IV & V programme and the lessons learned from tackling a computer network at Los Alamos. IV & V is required of compartmented and multilevel systems, and the functional properties which the process checks, as well as the process itself, are described. It is quite possible that problems with policy will be thrown up as well as technical matters.

034214 ‘The composition problem: an analysis’

G King, *NCSC 94 pp 292–298*

The main practical problem in security composition is not coupling two security products, but in composing a TCB with commerical off the shelf products, but this is not reflected in current research. The heart of the matter is the lack of standards for security relevant interfaces, protocols and data formats; this makes it very hard to compose trusted with untrusted products without modifying them and thus introducing unevaluated code into the security envelope.

034215 ‘Security in a Client Server Environment’

LG Lawrence, *Network Security (July 94) pp 5–15*

The author provides an overview of client-server computing, describes some of the technical and operational risks, and discusses the available technical controls, including OSF/DCE and Kerberos.

034216 ‘Self-authenticating proxies’

MR Low, B Christianson, *The Computer Journal v 37 no 5 (94) pp 422–428*

A technique is proposed for integrating authentication, access control and resource management in distributed systems. Each service generates proxies which act as capabilities and allow access to it; public key techniques are used to minimise the areas of trust, and proxies can be delegated either in serial or in parallel, the latter case allowing shared control of resources.

034217 ‘Covert Channels — Here to Stay?’

IS Moskowitz, MH Kang, *Compass 94 pp 235–243*

Capacity is not the only measure of a covert channel, as channels may exist which have a one-off capability to send a fixed number of bits and thus possess zero capacity. One should rather measure the longest message which can be transmitted under realistic assumptions. There are a number of trade-offs in minimising this, and various mechanisms including pumps may be useful.

034218 ‘Aggregation in relational databases: controlled disclosure of sensitive information’

A Motro, DG Marks, S Jajodia, *ESORICS 94 pp 431–445*

This paper proposes an approach to control disclosure of sensitive information through aggregation in relational databases. It is based on the use of views that define secrets which can be disclosed to a limited degree. Each view is assigned a threshold value that indicates the maximum number of tuples in the view which can be released, and the system tracks the number released to date to any given user.

034219 'Modern multilevel security (MLS): practical approaches for integration, certification and accreditation'

B Neugent, M Burgoon, J Firey, M Rudell, *NCSC 94 pp 309–317*

Significant numbers of multilevel secure systems are finally being fielded, and most of them are guards or workstations, The security of the latter depends on integrating commercial applications, which not only change frequently but often try to do things such as seizing the root window or the display colour map which the TCB will not allow. The US DoD's strategy is to build incrementally more complex systems by adding DMBSs, LANs and the like as time goes by, and by maintaining a registry of applications which run acceptably on multilevel systems. There is also an evolving set of accreditation precedents. However, tools are still needed which will monitor fielded systems and detect subtle errors in configuration.

034220 'An Experience Modeling Critical Requirements'

LN Paynes, AP Moore, DM Mihelcic, *Compass 94 pp 245–255*

The authors provide a security model for the External COMSEC Adaptor, a US encryption device which selectively encrypts classified information in a multilevel network, and discuss the lessons learned.

034221 'Database Security'

G Pernul, *Advances in Computers v 38 (1994) pp 1–72*

This is a survey article on database security, which encompasses a wide range of topics from the legal and societal framework of information processing to the mechanics of multilevel database implementation and covert channel suppression. The main results in the field are described, as are some early secure database products, and finally the author presents a unifying model for multilevel security.

034222 'On the validity of the Bell-LaPadula Model'

EEO Roos Lindgren, IS Herschberg, *Computers and Security v 13 no 4 (94) pp 317–333*

The authors describe the background to the development of the Bell-LaPadula security model, which they explain in some detail using the original notation. They then discuss some of the criticisms which have been made of it, such as the difficulties which may arise with the semantics of data and when considering dynamic changes in classification levels. They also discuss the practical difficulties which are caused by the *-property.

034223 'Issues Associated with Porting Applications to the Compartmented Mode Workstation'

HH Rubinovitz, *ACM SIGSAC v 12 no 4 (Oct 94) pp 2–5*

There are serious problems in getting commercial applications to run on multilevel secure systems. Access to files may be quite different; access control lists may need redesign; the labeling information displayed by trusted X may obscure some of the display; and problems arise when an application is upgraded because of a high level input.

034224 'A Three Tier Architecture for Role-Based Access Control'

RS Sandhu, H Feinstein, *NCSC 94 pp 34–46*

The authors present a model for role-based access control in databases. It lies between the discretionary and mandatory access models: role membership and permissions are mandatory, and made by the security administrator. It is based on the ANSI/SPARC three tier database model, but could be applied to other systems too.

034225 'Access Control: Principle and Practice'

RS Sandhu, P Samarati, *IEEE Communications Magazine v 32 no 9 (Sep 94) pp 40–48*

The authors discuss access control and its relationship with auditing. They cover access matrices, access control lists, capabilities, authorisation relations, mandatory and rôle-based policies, and administrative issues.

034226 'The Architecture of Triad: A Distributed, Real-Time, Trusted System'

EJ Sebes, N Kelem, TC Vickers Benzel, M Bernstein, E Cohen, J Jones, J King, DM Gallon, R Zacjew, *NCSC 94 pp 237–246*

The authors report on Triad, a realtime distributed multilevel system which has been built on top of TMach and aims to keep its B3 rating while adding realtime scheduling, interprocess communication and replication features. The principal design tradeoffs concerned the distributed propagation of security attributes and the identification of covert channels in the scheduling.

034227 'Supporting object-based high-assurance write-up in multilevel databases for replicated architecture'

RK Thomas, RS Sandhu, *ESORICS 94 pp 403–428*

This paper discusses the execution of write-up operations in multilevel databases. A replicated architecture is considered where a single level database exists for each security level, and contains all data at that level plus a replica of all data at lower levels. Write-up operations are needed to propagate changes to low level data to their replicas at higher levels for the purpose of maintaining consistency among replicas. Requirements for serial correctness in the replicated architecture are given and different scheduling strategies are proposed. The interplay between serial correctness, scheduling algorithms, and replica control is discussed.

034228 'Security issues for federated database systems'

B Thuraisingham, *Computers and Security v 13 no 6 (Dec 94) pp 509–525*

The author describes the issues involved in building a multilevel secure system from a number of cooperating but possibly heterogeneous databases. One can proceed either bottom-up (from evaluated components) or top-down (from requirements); various constraints and design issues are discussed.

3 Security Management and Policy

034301 'An Engineering Approach to Secure System Analysis, Design and Integration'
E Amoroso, WE Kleppinger, D Majette, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 40–51*

The authors describe AT & T's security engineering methodology. This starts from a systematic threat analysis and proceeds through the identification and integration of countermeasures.

034302 'TOPM: a formal approach to the optimization of information technology risk management'
KP Badenhorst, JHP Eloff, *Computers and Security v 13 no 5 (Oct 94) pp 411–435*

The authors present a formal model of risk management over the lifecycle of a system which uses portfolio management methods, and discuss it in the context of the controls in a bank teller support system.

034303 'The network memorandum of agreement (MOA) process: lessons learned'
WL Barker, LM Jaworski, GR Mundy, *NCSC 94 pp 459–467*

The authors describe the experience of negotiating security requirements for the US Defense Simulation Internet, whose nodes were accredited by a number of different agencies. It describes the management aspects of installing classified encryption devices on a substantial network; compliance with the accreditation process is assured by the NSA's not supplying key material until the paperwork has been completed.

034304 'Minimising Risk in Your Wide Area Network Design'
GP Bell, D Kavanagh, *Information Management and Computer Security v 2 no 3 (94) pp 26–28*

The authors discuss the options for providing resilience in wide area networks and for supporting disaster recovery sites efficiently.

034305 'Secure Auditing Means Better Business Protection'
P Berner, *Information Management and Computer Security v 2 no 4 (94) pp 32–34*

This article discusses Australia's Copyright Act and the organisation which represents software vendors. It exhorts firms to do regular software audits.

034306 'Making do with what you've got'
JW Berryman, BF Kennedy, *NCSC 94 pp 299–308*

The author discusses ways of enhancing C2 systems using physical, administrative and risk management techniques so as to meet some of the B1 trust goals. These techniques are illustrated for VAX/VMS systems.

034307 'Safety Aspects of Security Models'
T Beth, *Intelligent Systems: Safety, Reliability and Maintainability Issues, Springer NATO ASI series, pp 31–41*

The author discusses the interaction of safety, reliability and security, and identifies the maintainability of complex systems as the most important practical problem. One way forward may be building local resilience properties into subsystems.

034308 'The Quality and Security Debate - part 2'
CW Blatchford, *Computer Fraud and Security Bulletin (Sep 94) pp 7–14*

The author discusses the problems of classifying computer security abuses, packaging information security products, and ITSEC.

034309 'Accounting for PCs'
G Booth, *Banking Technology v 11 no 9 (Nov 94) pp 52–56*

The author claims that PC auditors can actually save the company money, by imposing control on hardware and software use as well as worrying about security.

034310 'On measurement of operational security'
S Brocklehurst, B Littlewood, T Olovsson, E Jonsson, *Compass 94 pp 257–266*

The authors encouraged students to attack a network of 22 workstations and a server, and studied how they went about it. The students attached a very high value to becoming root on the server, but there was also a considerable diversity of motivation: some students considered it rewarding to learn about system security, while others were satisfied with proving the feasibility of an attack rather than actually carrying it out.

034311 'Security technologies'
TA Brooks, MM Kaplan, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 4–8*

The authors provide an overview of communications security threats and countermeasures, as an introduction to a special journal issue on security.

034312 'Digital Signatures: Are They Legal for Electronic Commerce?'
PW Brown, *IEEE Communications Magazine v 32 no 9 (Sep 94) pp 76–80*

The author discusses whether digital signatures will be acceptable in US courts. From the point of view of legal principles, they should be; provided that the intent is there, a wide range of marks, stamps, seals and other devices have been recognised as having the effect of signatures in various applications. Digital signatures provide better technical protection, but there is no case law yet; indeed, there is very little case law on the broader topic of how people act through computers. However, US government funds have been disbursed without manual signatures since 1987. The conclusion is that digital signatures are usable, although their evidentiary effect remains to be tested.

034313 'Towards a National Public Key Infrastructure'
S Chokhani, *IEEE Communications Magazine v 32 no 9 (Sep 94) pp 70–74*

The author discusses the issues involved in setting up a public key infrastructure for the USA, such as the incompatibility of the standards proposed by CCITT X.509 and ANSI X9.30. Specific concerns include certificate revocation, the certificate hierarchy, how the root key is guarded, and the legal acceptability of the system.

034314 'MI5 to advise on IT security'
A Collins, *Computer Weekly (10 Nov 94) p 1*

The UK security service will in future advise government departments on computer security and investigate incidents. This has led to concern about privacy and data protection.

034315 'Suspicions surface about bugged Swiss encryption units'
Computer Fraud and Security Bulletin (Oct 94) pp 5–6

This article reports the Buehler affair. Hans Buehler, a former employee of a Swiss encryption equipment vendor, claims that the firm had been selling weak devices to overseas customers for at least 15 years at the behest of German and American intelligence. The product from this allegedly included Libyan diplomatic traffic related to the Berlin disco bombing, which led to the US raid on Tripoli; and Iranian diplomatic traffic which proved Iran's involvement in an assassination in Paris.

034316 'BDSG und # 203 Strafgesetzbuch'
Datenschutzberater (15 Nov 94) pp 1–4 (in German)

German law makes it a criminal offence for doctors, lawyers, tax advisers and auditors to reveal client data to unauthorised persons. It is argued that the use of PCs without special security measures could be illegal, and this is discussed at length in the case of doctors, who have an additional obligation to keep reliable records.

034317 'Schutzmassnahmen gegen PC-viren'
Datenschutzberater, 17 Oct 94 pp 9–12 and 15 Nov 94 pp 11–14 (in German)

This article describes the anti-virus advice from the BSI (the German federal information security agency), which encourages central reporting of incidents (to the BSI), describes basic recovery procedures and provides a glossary of terms.

034318 'Development history for procurement guidance using the trusted computer system evaluation criteria (TCSEC)'
ML De Vilbiss, *NCSC 94 pp 198–205*

This article describes the development of the NSA's procurement guidelines for secure computer systems. These were held up by a lack of understanding of how to apply the TCSEC to an integrated system, rather than just to components; as a result, they have been spilt into four volumes, of which three have been published and the fourth is due in 1995.

034319 'Key Escrowing Today'
DE Denning. M Smid, *IEEE Communications Magazine v 32 no 9 (Sep 94) pp 58–68*

The authors describe some of the mechanisms and supporting procedures of the US government's escrowed encryption standard, such as dual control, backup, and clearance requirements.

034320 'The security-specific eight stage risk assessment methodology'
DL Drake, KL Morse, *NCSC 94 pp 441–450*

The authors discuss a risk assessment methodology which takes into account the likely time lapse between an attack and its discovery, whether or not the attack is successful in breaking security.

034321 'Escrow Fraud: An Exploratory Study of a Neglected Crime'
J Doocy, D Schichor, *Journal of Security Administration v 17 no 1 (Oct 94) pp 18–36*

The escrow business in California involves about 1000 firms with over $1bn at risk at any one time. Fraud has become a serious problem: the business is complex, invisible and marketed through channels which expose it to temptation; there are problems with staff competence; a lot of money is involved, with the average fraud over $250,000; there is no effective central regulation or investigation; and when abuses take place, there is little public outcry.

034322 'Developing a Successful Network Disaster Recovery Plan'
B Edwards, *Information Management and Computer Security v 2 no 3 (94) pp 37–42*

The author discusses some approaches to developing a network recovery plan.

034323 'Software Auditing — Why, and How ...?'
D Fessey, *Computer Audit Journal v1 (94) pp 12–20*

Software auditing — ensuring that an organisation takes reasonable steps to control software piracy — can bring unexpected benefits such as releasing vast amounts of disk space and slashing support costs. There are also some intricate legal complications which can arise with corporate acquisitions and mergers.

034324 'A Security Framework for Information Systems Outsourcing'
D Fink, *Information Management and Computer Security v 2 no 4 (94) pp 3–8*

When outsourcing the development or operation of information systems, a firm should keep its policymaking, quality and security functions in-house.

034325 'Establishing Security in a Multi-platform, Multi-vendor, Enterprise-wide IT Environment'
KJ Fitzgerald, *Information Management and Computer Security v 2 no 4 (94) pp 9–15*

The author describes a number of the security problems which arise in firms which downsize from mainframes to distributed systems. He mentions a number of possible solutions, including Kerberos, OSF/DCE and NetSP.

034326 'Security and Network management: Changes in the Way We Work'
KA Forcht, YWA Tsai, *Information Management and Computer Security v 2 no 4 (94) pp 35–41*

The authors discuss the security implications of outsourcing network management and point out that some LAN management products can provide useful points of control.

034327 'The electronic intrusion threat to national security and emergency preparedness telecommunications: an awareness document'
J Frizell, T Phillips, T Groover, *NCSC 94 pp 378–399*

This paper assesses the threat posed by phone phreaks, hackers and the like to US government communications. A number of case histories of outside attacks are discussed, as is the lack of information on abuses by insiders and by foreign intelligence services. Nonetheless, hackers have shown the capability to monitor both voice and data traffic remotely, and to alter network databases so as to forward calls, turn off biling and create unauthorised accounts.

034328 'Digital Signatures and Their Uses'
MJ Ganley, *Computers and Security v 13 no 5 (Oct 94) pp 385–391*

The author provides a management level introduction to digital signature algorithms. He describes both RSA and DSA and mentions some key certification issues.

034329 'Sniffing in the Sun: History of a Disaster'
S Gordon, I Nedelchev, *Network Security (July 94) pp 16–19*

The authors describe the February 1994 password snarfing attack on the Internet, and provide 'commentary' from some of the alleged hackers which indicates that part of the motivation was the desire for media attention. They also describe how the program worked.

034330 'Internet Firewalls'
WM Hancock, *Network Security (Aug 94) pp 10–11*

The author provides a management level overview of three types of Internet firewall: the packet filter, the circuit gateway and the application gateway.

034331 'Issues and Problems in Secure Remote Access'
WM Hancock, *Network Security (June 94) pp 14–18*

The author discusses some of the problems in securing dial access to corporate systems, and recommends using a gateway machine which can support a range of authentication methods.

034332 'Can wiretaps remain cost-effective?'
R Hanson, *Communications of the ACM v 37 no 12 (Dec 94) pp 13–15*

The cost of providing a wiretap capability in a modern digital network is high, and if mandated in the USA could cost from \$2.5bn to \$5bn in the first four years alone, according to phone companies. Although FBI claims suggest a marginal economic benefit of the order of \$1bn a year from wiretaps, police agencies only spent \$51.7 million. In fact, three states forbid wiretaps completely; 29 others did not use any; and 73% of state wiretaps were in New York, New Jersey and Florida. It is concluded that forcing phone companies to subsidise wiretaps makes no more sense than forcing helicopter companies to sell at a loss to the police.

034333 'How Secure Is Data over the Internet?'
HJ Highland, *Network Security (June 94) pp 9–11*

The author summarises forty two security points about the Internet drawn from Cheswick and Bellovin's book (*see reviews section*).

034334 'Partitioning the security analysis of complex systems'
H Holm, *NCSC 94 pp 283–291*

The author discusses the relationship of the trusted computing base to real world notions of trust in a number of environments, including universities, hospitals and the DoD. For example, a system might be subverted so as not to invoke the TCB; and there are many other practical problems in making TCSEC concepts apply to real systems.

034335 'Virus Control on networks: Solving the Unsolvable'
J Hruška, *Network Security (Sep 94) pp 10–13*

Controlling a network's exposure to viruses means minimising write/create access rights as well as having a virus detection system, which should be based on the server rather than on the workstations.

034336 'Information highway security'
RV Jacobson, *Information Security Monitor v 9 no 11 (Oct 94) pp 5–7*

The author describes the history of the Internet and its predecessor the ARPAnet, and goes on to discuss some of the commoner hacking techniques, firewalls and the CERT.

034337 'A taxonomy for security standards'
WA Jansen, *NCSC 94 pp 165–174*

US DoD security standards fall into two broad categories. The first, the standards for uniformity, cover the interchangeability of products and personnel, the latter being achieved through standard interfaces such as POSIX and SQL. The second category, the standards for quality, can be either assessment procedures or documents covering matters such as terminology and methods.

034338 'EC developments in IT law'
D Jerrard, H Small, M Crichard, *Computer Law and Security Report v 10 no 5(Sep/Oct 94) pp 250–255*

The authors tabulate the various legislative processes under way in Brussels which could affect European IT businesses, including those concerning IPR, data protection and ITSEC issues.

034339 'Data Integrity'
S Kirk, M Hogg, *Information Security Monitor v 9 no 10 (Sep 94) pp 5–7*

The authors consider the integrity requirements of Britain's Data Protection Act and the due diligence guidelines in the DTI Code of Practice. They describe some of the technical mechanisms that can be used.

034340 'Marketing and Customer Service in Security programmes'
AR Krull, *Computer Fraud and Security Bulletin (Oct 94) pp 7–16*

The author discusses how to go about selling security in a modern distributed organisation; the key is being perceived to provide good service.

034341 'Software piracy and corporate compliance: an introduction'
SI Kyer, *Computer Law and Security Report v 10 no 5 (Sep/Oct 94) pp 245–246*

The author surveys the software piracy situation in Canada and presents a model corporate software policy.

034342 'Comments on a paper by Voas, Payne and Cohen: "A model for detecting the existence of software corruption in real time" '
P Ladkin, H Thimbleby, *Computers and Security v 13 no 6 (Dec 94) pp 527–531*

The authors criticise a paper on virus detection on the grounds that it assumed the existence of protected mode multitasking operating systems, while most viruses affect DOS machines.

034343 'Stopping the copy cat crimes'

A Lawrence, *Computer Business Review v 2 no 9 (Sep 94) pp 18–20*

This article surveys PC software piracy in a number of countries. In Italy, government action against pirates has boosted sales by 88% from 1992 to 1993; elsewhere, the industry focuses on education. While some smaller firms use dongles, larger firms give various reasons for not using them; but all highlight the hassle factor for users.

034344 'IT Security Standards and the Adoption of a Benchmarking Approach'

T Lillywhite, *Computers and Security v 13 no 6 (Dec 94) pp 467–471*

The author describes some of the many international standards bodies and argues that benchmarking based on the DTI Code of Practice is more relevant to the needs of real organisations.

034345 'Administration Initiates Dialog on Cryptography Policy'

S Lipner, *Data Security Letter no 52 (Sep 94) pp 1–4*

The author summarises recent political activities in the USA over escrow encryption and related issues. It gives a brief synopsis of two meetings of a working group which brings together government, industry and academics.

034346 'Integrity In Information Systems - Executive Summary'

W List, R Melville, *Computers and Security v 13 no 4 (Sep 94) pp 295–301*

People tend to trust computer output, yet it is not practical to demonstrate at all times that the output is true. On the other hand, it is not acceptable if one can never make such a demonstration. The authors propose that systems should be so designed that data items are timestamped, visible error detection mechanisms are incorporated and users are empowered to supervise the business process.

034347 'EC Information Security Legislation: Where Now?'

W London, *Computer Law and Security Report v 10 no 5 (Sep/Oct 94) pp 226–233*

The author reviews the harmonisation of EC information security laws and discusses whether these constitute an impediment to the single market. Laws vary widely, and cover misuse, IPR and/or data protection and privacy issues. Complying with them can be a burden, and the diversity also lets firms seek out data havens. A number of future options are discussed, including making either incident reporting or insurance mandatory and imposing a specific duty of care on companies.

034348 'Norwegian encryption standard moves forward'

W Madsen, *Computer Fraud and Security Bulletin (Nov 94) pp 10–12*

The Norwegian government has introduced its own encryption standard called NSK, which was developed by the ministry of defence, Norwegian Telecom and a parastatal defence contractor. It uses a secret algorithm in a tamperproof chip and instead of a key escrow system there will be tight licensing, with sales limited to defence contractors and bona fide data protection applications. In addition, Norwegian Telecom will manage the keys of the line encryptors using these chips and will be able to provide access to the intelligence services.

034349 'Senate Hearings on Fraud in the IRS'

W Madsen, *Computer Fraud and Security Bulletin (Nov 94) pp 8–10*

Electronic filing of tax returns in the USA has led to systematic tax fraud to the point that the facility may have to be suspended; a number of schemes are described. Privacy violations by IRS employees are also a problem.

034350 'White House Denies Clipper Will Become Mandatory'

W Madsen, *Computer Fraud and Security Bulletin (Dec 94) pp 6–7*

A White House policy analyst denied in November that the FBI director had publicly favoured outlawing non-escrowed encryption. This denial was ridiculed by people who had transcripts of the director's speech.

034351 'Marketing public sector information: some issues'
T Mandeville, DM Lamberton, S Macdonald, *Computer Law and Security Report v 10 no 5 (Sep/Oct 94) pp 234–237*

The authors discuss the marketing of government information, both official and illicit, from the point of view of economics.

034352 'Keeping out intruders'
E Mansell-Lewis, *Computer Weekly (10 Nov 94) p 1*

The author reports the opinions of a number of industry figures on the security implications of the growth in networking; the consensus is that management aspects are most important as most breaches result from errors.

034353 'Software Copyright Infringement'
A Maughan, *Computer Fraud and Security Bulletin (Oct 94) pp 16–17*

The author discusses a recent case, Ibcos Computers Ltd vs Poole, in which it was held that a former employee could infringe copyright from memory, and that copyright subsisted in a whole program rather than just its components.

034354 'A methodology to include computer security, safety and resilience requirements as part of the user requirement'
DNJ Mostert, SH von Solms, *Computers and Security v 13 no 349–364*

Introducing security and safety requirements as an afterthought is not effective; they must be introduced when a system is specified. A method for doing this is presented, and discussed in the context of an air traffic control system.

034355 'Effectiveness of Passwords'
S Ongetta, *Network Security (Aug 94) pp 14–17*

The author discusses password management, and how a firm's culture can interact badly with software access controls.

034356 'Protecting Information in the PC'
S Ongetta, *Computer Fraud and Security Bulletin (Nov 94) pp 17–19*

The effectiveness of PC security tools depends so critically on how well they are used that awareness training should be the main priority.

034357 'Demonstrating the elements of information security with threats'
DB Parker, *NCSC 94 pp 421–430*

The author discusses a number of computer cases including attempted extortion, abuse of encryption by a criminal, omission of accountancy software, and ATM fraud. He uses them to draw distinctions between integrity and authenticity, confidentiality and possession, and so on.

034358 'Single Sign-on - What Is It? What Are The Requirements?'
T Parker, *Information Security Monitor v 10 no 1 (Dec 94) pp 5–9*

The author describes how some products allow single sign-on to a range of applications, and the various additional threats which this introduces. Ideally these products should have a Kerberos-like crypto interface to applications, but more often they are just scripting shells which remember and invoke a number of conventional logon sequences.

034359 'Benchmarking'
G Penfold, *Computer Audit Update (Nov 94) pp 10–16*

The author considers how auditors can benchmark the effectiveness of IT controls and reports a system which was piloted on 65 audit clients.

034360 'The Fortress Mentality: Its Time Has Come Again'
P Peterson, *Network Security (June 94) pp 12–13*

This article describes some of the risks run by businesses which use the Internet, from password snarfing attacks through corporate embarrassment.

034361 'The Fortress Mentality - Part II: The Internet'
P Peterson, *Network Security (Aug 94) pp 11–14*

The author presents a management level overview of the TCP-IP protocol used in the Internet and explains some of its security problems.

034362 'Security Awareness and the Persuasion of Managers'
DF Poindexter, *NCSC 94 pp 451–458*

The author discusses the organisational constraints on security awareness programmes in terms of Richard Pascale's theory of the controls which social structures place on individuals' ability to cause change. The principles he derives enable one to spot organisations which are so resistant to change that a sensible security person would resign and seek work elsewhere.

034363 'Data Interchange and Legal Security — Signature Surrogates'
K Rihaczek, *Computers and Security v 13 no 4 (Sep 94) pp 287–293*

The author discusses some of the pitfalls in having a digital signature or other technical surrogate for a manuscript accepted by a court. The court might not accept such a signature, or might not understand it, or a user might be tricked by an insecure application, even though the signature mechanism itself were sound. He propounds a number of principles, such as that the signatory must be warned before signature that he is about to change his legal status, and that the signed text should be directly visible to him at this time. These ergonomic factors may be more important in law than the cryptographic security of the signature algorithm itself.

034364 'Security is as simple as one ... two ...'
WD Riley, *Computer Fraud and Security Bulletin (Dec 94) pp 16–19*

The author discusses how the military model of classifications and clearances was applied to a commercial environment and gives details of the four levels used. The security level determined various parameters including backup rules, password length and whether dial access was allowed.

034365 'preventing Software Piracy'
R Schifreen, *Network Security (Sep 94) pp 17–19*

The author discusses some of the techniques used by software vendors to catch software pirates, such as statistical analysis of support calls, and the audit techniques which organisations can use to detect piracy among their staff.

034366 'What motivates a hacker?'
R Schifreen, *Network Security (Aug 94) pp 17–19*

Hackers may have a wide range of motives - from curiosity, boredom or the desire for a challenge through to greed or revenge.

034367 'Network Security In a Heterogeneous Environment'
RL Sharp, SR Eisen, WE Kleppinger, ME Smith, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 52–60*

The authors describe a AT & T methodology for protecting networks. This involves defining trust domains, selecting mechanisms such as firewalls or encryption devices, and integrating them into solution.

034368 'Can computer crime be deterred?'
S Sherizen, *NCSC 94 pp 412–320*

Empirical studies have shown that criminals do not react rationally to deterrence. One may speculate that computer criminals are more rational than most, but there is really not enough evidence to be sure.

034369 'Security in the client/server environment'

J Sherwood, J Fitzgerald, *Computer Fraud and Security Bulletin (Dec 94) pp 8–16*

The authors discuss some of the new security problems which are introduced by a move to client-server computing. The mainframe security model breaks down; integrating the access control subsystems of a diverse server population is hard; available PC operating systems are insecure; and there are problems with the atomicity of database transactions, the granularity of access control, the respective rôles of the database and the application, and the overall administration.

034370 'Security Guidelines in Information Technology for the Professional Practitoner'

R Sizer, *Supplement to Computer Law and Security Report v 10 no 5 (Sep/Oct 94)*

This booklet provides guidelines - in effect, an extended checklist - for the due diligence which might be expected of a professional firm such as a law office in respect of its internal computer security. In addition to a 14 page guide to security terminology, threats and countermeasures, it provides a list of the relevant ISO standards.

034371 'Making Security Pay'

M Smith, *Computer Fraud and Security Bulletin (Nov 94) pp 12–17*

The author discusses how to turn an organisation's security team from a cost centre into a profit centre. For this to happen, the security manager needs to be a good salesman, and he needs to be able to quantify benefits such as reduced stock shrinkage.

034372 'Security Evaluation Criteria'

L Strous, *Computers and Security v 13 no 5 (Oct 94) pp 379–384*

The author sets out the position taken on security evaluation criteria by the security SIG of the Dutch Computer Society. These have to do different things at different levels (system, product, component, etc).

034372 'Security in Distributed and Client/Server Systems - A Management View'

IM Symonds, *Computers and Security v 13 no 6 (Dec 94) pp 473–480*

The authors discusses the management concerns raised by distributed computing environments. Not only is central control weakened - and sometimes even made impossible - but there are growing numbers of outside communications links which bring complex vulnerabilities. It is increasingly prudent to have a strong policy framework.

034373 'Privacy and the Internet: The next step'

F Türkheimer, *Computer Networks and ISDN Systems v 27 no 3 (Dec 94) pp 395–401*

The author gives a legal perspective on Internet privacy. This is complicated, as the net has no rules or responsible officers, and is spread over at least 146 countries with widely varying privacy laws. He discusses these for the six main countries (the USA, Canada, France, Germany, the UK and Japan) as well as for the EC, and touches on the issue of employer access to employee email.

034374 'Towards Understanding Evolving Security Threats: Entrepreneur, Vigilante or Terrorist?'

BM Turner, *Journal of Security Administration v 17 no 1 (Oct 94) pp 5–17*

The author discusses post-Soviet terrorist threats to US interests. Muslim fundamentalist groups are the most obvious worry, but domestic minority tensions also have the potential to spawn terrorists or vigilantes: black Muslim groups have used force to clean up neighbourhoods, while neonazis, extreme zionists and other such groups also bear watching.

034375 'Interception of communications for criminal investigation - a comparative analysis'

IE Vassilaki, *Computer Law and Security Report v 10 no 5 (Sep/Oct 94) pp 238–241*

Law enforcement interception of fax, email and similar communications can give rise to legal problems. Some states forbid it explicitly, while others allow it; and jurisdictional difficulties arise from the increasingly international nature of electronic communications. Some countries, such as Switzerland, have laws which allow telephone tapping but which may not extend to other media. In others, access to email may count as search rather than interception; and in Britain, only public networks may be tapped. Both the OECD and the EC are making attempts to harmonise matters.

034376 'Policing Policies'

L Warren, *Computer Weekly (27 Oct 94) pp 52–53*

The author discusses the differing views which users and IT professionals have of data security, and quotes the views of a number of industry figures on the subject.

034377 'Remote Controls'

L Warren, *Computer Weekly (10 Nov 94) p 50*

The author discusses portable PC security: defence sector purchasers are starting to insist on security features, including removable hard disks, and a number of products are briefly described.

034378 'New Initiatives Which May Erode Your Privacy: Or George Orwell Was Off by Only a Decade'

KP Weiss, *Information Management and Computer Security v 2 no 3 (94) pp 43–45*

The author opposes the Clipper initiative on the grounds of rights erosion, cost to business, and lack of effectiveness.

034379 'The Data Network Disaster Recovery Plan: Considerations and Concerns'

S White, *Information Management and Computer Security v 2 no 3 (94) pp 29–36*

A proper map of the corporate network is an important tool not just in spotting single points of failure but in selling the concepts of network resilience and recovery to management.

034380 'Cost Effectiveness of Anti-Viral Scanners'

BP Zajac, *Computers and Security v 13 no 5 (Oct 94) pp 392–400*

The author explains how to calculate the net present value and expected rate of return of an investment in anti-virus software. Using Kephardt and White's figure of 0.00042 for the probability that a given PC in a large organisation will be infected in any one year, a typical anti-virus program with a purchase price of \$136 and an annual maintenance fee of \$100 is not cost-effective unless the cost of each attack is over a million dollars.

4 Formal Methods and Protocols

034401 'Maintaining Security in the Presence of Transient Faults'
R Canetti, A Herzberg, *Crypto 94 pp 425–438*

If we have a number of authentication servers, and an enemy who can penetrate any of them but who does not have the resources to penetrate them all at once, then how can we maintain security? The authors demonstrate a protocol in which each user shares a secret with each server, and the secrets are refreshed by hashing at the end of each round. This can recover security so long as there is always at least one uninfected server, and at least one secure communications link between one server uninfected in round m and another which is uninfected in round $m + 1$. These conditions are the weakest possible.

034402 'Cryptanalysis of the Gemmell and Naor Multiround Authentication Protocol'
C Gehrmann, *Crypto 94 pp 121–128*

A multiround authentication protocol which was based on error-correcting codes is shown to be vulnerable to an impersonation attack whenever the number of rounds is even.

034403 'Privacy Enhanced Mail Design and Implementation Perspectives'
DF Hadj Sadok, T Kelner, *Computer Communication Review v 24 no 3 (July 94) pp 38–46*

The authors discuss some of the problems of PEM, including the management of certificate revocation lists, the lack of correspondence between a certification authority's name and address (and indeed between distinguished names and Internet addresses generally), the use of a single certificate for both encryption and signature, error reporting, and the interface to electronic notary services.

034404 'Recursive mappings for computer virus'
XA Li, JH Fu, YG Song, HY Yang, *Chinacrypt 94 pp 279–286 (in Chinese)*

This paper builds on Adleman's suggested definition of computer viruses in terms of Gödel numberings, and suggests a recursive mapping definition. They show that programs exist which are viruses under their definition but not Adleman's and vice versa; and that for any virus, there exists a program which it cannot infect or injure.

034405 'Forging a Clipper Message'
M Lomas, M Roe, *Communications of the ACM v 37 no 12 (Dec 94) p 12*

Since the AT & T secure telephone uses Clipper in output feedback mode, an attack in depth can be used to forge an encrypted call. This diminishes the evidential value of Clipper decrypts.

034406 'Effect of key generators on the automatic search for flaws in key management schemes'
D Longley, S Vasudevan, *Computers and Security v 13 no 4 (Sep 94) pp 335–347*

The authors consider the effects which poor key generation may have on formal techniques for validating key management schemes and other cryptographic protocols; these methods may not find attacks involving multiple invocations of a key generator whose outputs may possess some mutual correlation or other relationship. They discuss how their protocol tester can be extended to deal with key generators.

034407 'Kerberos: An Authentication Service for Computer Networks'
BC Neuman, T Ts'o, *IEEE Communications Magazine v 32 no 9 (Sep 94) pp 33–38*

The authors describe the Kerberos authentication system and discuss its strengths and weaknesses. They describe the software which implements it, and some of the features of the later releases such as GSSAPI and the forthcoming introduction of public key cryptography.

034408 'On the Specification, Validation and Verification of Security in Access Control Systems'
G O'Shea, *The Computer Journal v 37 no 5 (94) pp 437–448*

The author discusses how to go about verifying an access control system of the Clark-Wilson type, and presents a formal model based on sets of subjects, objects and rights. He shows that the general problem of validating a policy in this model is NP-complete, and that specific subproblems inhabit a range of complexity classes.

034409 'Using a semiformal security policy model 2C a C2 better'
M Schaefer, GR Grossman, JJ Epstein, *NCSC 94 pp 153–164*

The authors developed a semiformal policy model for Trusted NetWare and describe how it handles the product's directory services, which are Novell's implementation of X.500. The exercise showed that such models are useful tools, even at lower levels of assurance where their use is not mandatory. In fact, discretionary policies are often more complex than mandatory ones and can benefit more: a formal modeling exercise establishes whether policy concepts are well-defined and complete, and forces correspondences to be made explicit.

034410 'Secure Distributed Computing'
JI Schiller, *Scientific American (Nov 94) pp 54–58*

The author describes Project Athena, which developed the MIT campus network and led to the development of the Kerberos authentication protocol suite. The architectural concepts of Kerberos are described in some detail: the key distribution centre and ticket granting service are the heart of the system, and they respectively check passwords and manage access rights. Later versions may include public key features to expand the user base from tens of thousands to millions.

034411 'Cryptanalysis and Protocol Failures'
GJ Simmons, *Communications of the ACM v 37 no 11 (Nov 94) pp 56–65*

The author describes a protocol by Tatebayashi, Matsuzaki and Newman and shows how to break it: two users who collude can use the server as a decryption oracle. He also shows that when a certain interactive protocol is used to generate message keys for the digital signature algorithm, in order to suppress the previously known covert channels, there arises yet another covert channel — called the cuckoo's channel — which the signer's partner in the protocol can use to communicate with third parties. He concludes by discussing the principles of protocol analysis.

034412 'Subliminal Channels; Past and Present'
GJ Simmons, *European Transactions on Telecommunications v 5 no 4 (Jul/Aug 94) pp 459–473*

This paper describes a protocol proposed in 1978 to monitor compliance with the SALT II treaty, and how the author found a potentially disastrous flaw in it — a subliminal channel which would have allowed the USSR to discover which Minuteman silos contained missiles. This discovery led to his subsequent work on the topic of subliminal channels, some of which is described. In particular, channels in the ElGamal and DSS digital signature scheme are compared, and it is shown that the DSS provides the most hospitable setting for subliminal communications discovered to date.

034413 'Secure Timeliness: On the Cost of Non-Synchronised Clocks'
R Yahalom, *Computing Systems Usenix v 7 no 4 (Fall 94) pp 451–465*

Many protocols, including Kerberos, rely on clocks to establish message freshness. However, relaxing the assumption that the clocks are synchronised may be cheap. For example, an n-domain authentication protocol with trusted clocks needs $n+3$ messages, but this rises to only $n+4$ if clock synchronisation can no longer be assumed.

034414 'Towards a Formal Verification of a Secure and Distributed System and Its Applications'
C Zhang, R Shaw, MR Heckman, GD Benson, M Archer, K Levitt, RA Olsson, *NCSC 94 pp 103–113*

The authors describe the formal verification of Silo, a system consisting of a collection of connected microprocessors, a distributed operating system and a compiler. The verification is being done with HOL and has so far been completed for a subset of the system with a simplified instruction set and static process naming. They discuss the problem of designing a distributed message passing kernel and a compiler so that they can be verified, despite the fact that no canonical equivalence exists between the parallel machine's behaviour and the programming language semantics. The goal is to show that any application which is proved correct in Hoare logic will run correctly on the system.

5 Secret Key Algorithms

034501 'The Security of Cipher Block Chaining'
M Bellare, J Killian, P Rogaway, *Crypto 94 pp 341–358*

If a block cipher is a random oracle, then so is the message authentication code derived from it using cipher block chaining on a certain number of input blocks, since any means of distinguishing the MAC from a random function could be carried down to the cipher itself. Thus if the cipher is strong, we can expect that its MAC is too, at least for input strings of fixed length.

034502 'Cryptanalysis of Cryptosystems based on Remote Chaos Replication'
T Beth, DE Lazic, A Mathias, *Crypto 94 pp 318–331*

The authors show how to attack an analogue encryption scheme proposed by Chua, which depended on the use of synchronised chaotic oscillators, by using signal processing techniques.

034503 'Bounds for Resilient Functions and Orthogonal Arrays'
J Bierbrauer, K Gopalakrishnan, DR Stinson, *Crypto 94 pp 247–256*

An (n, m, t)-resilient function has n-bit inputs, m-bit outputs and the property that with any t input bits fixed, each output m-tuple is still equally likely. A linear code of distance d gives a resilient function with $t = d - 1$, and this coding relationship can be used with linear programming techniques to provide a simpler proof of Friedman's bound on the size of t.

034504 'New Types of Cryptanalytic Attacks Using Related Keys'
E Biham, *Journal of Cryptology v 7 no 4 (Autumn 94) pp 229–246*

This is the journal version of the author's paper (**023504**) which explains the rôle of key scheduling in block ciphers and shows how to break those, such as Lucifer and LOKI, whose key schedules are too regular. There are two types of attack: chosen plaintext attacks, and the novel 'chosen key' attacks in which we have texts enciphered under the target key and also under variants of it. These can be used to construct characteristics in some ciphers which are independent of the number of rounds.

034505 'A Generalisation of the Discrete Fourier Transform: Determining the Minimal Polynomial of a Periodic Sequence'
SR Blackburn, *IEEE Transactions on Information Theory v 40 no 5 (Sep 94) pp 1702–1704*

The author generalises the Games-Chan algorithm to provide a Fourier transform algorithm for determining the minimal polynomial of a sequence in an arbitrary finite field. This uses Blahut's theorem on the weight of a sequence's spectrum.

034506 'Some cryptographic properties of exponential functions'
XG Chang, ZD Dai, G Gong, *Chinacrypt 94 pp 41–47 (in Chinese)*

This paper studies certain cryptographic properties of exponential functions over the finite field $GF(2^n)$. These functions provide permutations on an n-dimensional linear space which are easy to implement. The authors discuss their properties: they prove that exponential functions have an all-direction completeness property, exhibit a class of exponential functions satisfying the strict avalanche criterion, and prove that functions satisfying this criterion have high topological non-linear degrees. Finally, the non-linear degrees of exponential functions are discussed.

034507 'Attack on the Cryptographic Scheme NIKS-TAS'
D Coppersmith, *Crypto 94 pp 295–307*

The author shows how a noninteractive identity-based conference key sharing scheme proposed by Tsujii, Araki and Sekine can usually be broken by a relatively small number of collaborators.

034508 'A multiloop Vigenère cipher with exceptionally long component series'
WJ Corcoran, *Cryptologia v XVIII no 4 (Oct 94) pp 356–371*

The author proposes strengthening the Vigenère cipher by replacing the keyword with a linear congruential generator.

034509 'Some Results on a Classification and Enumeration of Matrices'
PR Feng, RJ Tao, *Chinacrypt 94 pp 214–224 (in Chinese)*

This paper discusses the application of Latin squares to cryptography, and in particular a combinatorics problem raised in the study of generating linearly independent Latin squares. Equivalence relations and canonical forms are introduced, and equivalence classes of n by n matrices over $GF(2)$ of rank n, $n-1$ and $n-2$ are counted.

034510 'Dickson Polynomials and Irreducible Polynomials over Finite Fields'
SH Gao, GL Mullen, *Journal of Number Theory v 49 no 1 (Oct 94) pp 118–132*

The authors provide necessary and sufficient conditions for $D_n(x,a)+b$ to be irreducible over $GF(q)$, where $D_n(x,a)$ is a Dickson polynomial. Dickson polynomials can also be used to generate optimal normal bases.

034511 'Constructing high dimensional linearly independent latin arrays from low dimensional arrays'
XA Gao, *Chinacrypt 94 pp 232–237 (in Chinese)*

This paper presents a new algorithm to construct a class of high dimensional linearly independent permutations from lower dimensional ones which is based on Latin array results by Tao and Chen. Its complexity is 2^{3r} where the starting permutation has order 2^r.

034512 'Automated Cryptanalysis of Transposition Ciphers'
JP Giddy, R Safavi-Naini, *The Computer Journal v 37 no 5 (94) pp 429–436*

The authors used digram frequences and simulated annealing techniques to solve transposition ciphers. A number of test results are reported for cipher lengths of 100–1000 characters and period lengths in the range 10–50.

034513 'A Chosen Plaintext Attack of the 16-round Khufu Cryptosystem'
H Gilbert, P Chauvaud, *Crypto 94 pp 359–368*

Naïve differential attacks on Khufu are prevented by the fact that its S-boxes are secret; however, there exist structures which cancel after eight rounds and these can be found using structures of chosen texts. The overall cost of the attack is 2^{43} chosen texts and computations, but some key information will start to leak after 2^{31} chosen texts and computations.

034514 'Cascaded GMW-form permutation polynomial sequences'
G Gong, *Chinacrypt 94 pp 180–185 (in Chinese)*

This paper constructs a new class of permutation polynomials of $GF(q^n)$ using the cascaded GMW polynomial from $GF(q^n)$ to $GF(q)$. This generates a new class of sequences over $GF(q^n)$ whose component sequences are cascaded GMW sequences over $GF(q)$.

034515 'On Linear Complexity of Periodic Sequence with Period p^n or p^n-1, p a Prime'
K Imamura, *Chinacrypt 94 p 186*

The author announces that the linear complexity of a sequence of period p^n over $GF(p)$ is no more than $p^{n-1}+1$, and that this bound is strict. More complex bounds are given for period p^n-1 over $GF(p^m)$, $m<n$.

034516 'Spectral Characteristics of Partially-Bent functions'
CH Jin, *Chinacrypt 94 pp 48–51*

This paper studies the effect that invariant linear structures have on the Walsh spectrum of a Boolean function, and obtains several new equivalent conditions under which a Boolean function is partially bent. Based on this, the author characterises the balance and linear structures of partially bent functions via their spectra.

034517 'Linear Cryptanalysis Using Multiple Approximations'
BS Kaliski, MJB Robshaw, *Crypto 94 pp 26–39*

The authors consider the effect on linear cryptanalysis of using multiple approximations. Each of these gives an essentially independent guess for a keybit, and formulae can be derived for the reduction in the data requirement: if we have n equally good approximations, we save a factor of n. Experiments were conducted on 5-round DES and a reduction of 50% was established.

034518 'An algorithm for the complete automated cryptanalysis of periodic polyalphabetic substitution ciphers'
JC King, *Cryptologia v XVIII no 4 (Oct 94) pp 332–355*

This article describes software designed to solve Vigenère ciphers. It uses the index of coincidence to find the key period, followed by probabilistic relaxation techniques to reconstruct the cipher alphabets.

034519 'On the excess of Hadamard matrices'
C Koukouvinos, *Utilitas Mathematics v XLV (1994) pp 97–101*

The author exhibits two families of Hadamard matrices, one of which has weights related to Golay sequences.

034520 'LFSR-Based Hashing and Authentication'
H Krawczyk, *Crypto 94 pp 129–139*

The author proposes a new way to use linear feedback shift registers to hash data: where the i-th data bit is equal to 1, accumulate the i-th shift register state. This is called Toeplitz hashing. He also proposes a method based on cyclic redundancy checks. These are both intended for use with one-time pad systems, and have the property that $h(M_1 \oplus M_2) = h(M_1) \oplus h(M_2)$.

034521 'Differential-Linear Cryptanalysis'
SK Langford, ME Hellman, *Crypto 94 pp 17–25*

By combining elements of both differential and linear cryptanalysis, the authors provide an algorithm which recovers 10 keybits 89% of the time from 8-round DES using only 512 chosen plaintexts, compared with the 5,000 required for differential and 500,000 needed for linear analysis. The basic idea is to find pairs of partity relations which either both hold or both fail.

034522 'Distribution of crosscorrelation function values of No sequences'
C Li, *Chinacrypt 94 pp 187–192*

No and Kumar defined "No sequences", which generalise GMW and Kasami sequences. Here the author discusses their cross-correlation properties. He proves that their cross-correlation function must lie within certain bounds, and indeed take on every value in the set $\{2^n-1, -2^m-1, -1, 2^m-1\}$ for suitable m and n. He also proves that the value 2^n-1 will appear 2^m times, -2^m-1 will appear $2^m(2^m-1)+(2^n-2)2^m(2^{m-1}-1)$ times, -1 will appear $(2^n-2)2^m$ times, and the value 2^m-1 will appear $(2^n-2)2^{n-1}$ times.

034523 'Criterion for the Nonsingularity of Feedback Shift Registers'
C Li, DQ Xie, *Chinacrypt 94 pp 147–154 (in Chinese)*

This paper presents a comprehensive set necessary and sufficient conditions for non-singularity of feedback shift registers of degree at most three over finite fields.

The results for $GF(2^m)$, $GF(3^m)$, and $GF(p^m)$ are slightly different, but the general pattern is that $f(x_1, x_2, ...x_n)$ will only generate a maximal sequence if f is a sum of certain powers of x_1 times linear or quadratic functions of the variables x_1 through x_n.

034524 'Necessary and sufficient conditions for correlation-immunity of multivalued logical functions'

SQ Li, BS Zeng, *Chinacrypt 94 pp 257–264 (in Chinese)*

This paper gives equivalent necessary and sufficient conditions for P-valued functions to have correlation-immunity when $P \geq 3$ is prime or $P = 4, 6$ using cyclic spectrum techniques. This paper also extends the Xiao-Massey results for $P \geq 3$.

034525 'Asymptotic estimation of the maximum order complexity of random sequences'

YZ Lian, SY Shen, *Chinacrypt 94 pp 274–278 (in Chinese)*

This paper studies the length of the shortest shift register which can generate a sequence a^n of length n, which is called the maximum order complexity and written $C(x^{(n)})$. This behaves like $2 \log n$, where base of the logarithm, q, is the number of possible values of the a_i. In particular, $C(x^{(n)})/2 \log n \to 1$ in probability, and for any $\lambda \in [0, 2)$, the expected maximum order complexity $E\{C(x^{(n)})\} \leq \lfloor 2 \log(n - \lambda \log n + 1)$.

034526 'Letter to the Editor'

J Lindballe, *Computers and Security v 13 no 4 (Sep 94) pp 303–305*

The author attacks a previously published article on the grounds that it did not distinguish effectively between free-start and target attacks for finding collisions.

034527 'Gröbner Bases and Linear Recurring Arrays'

ML Liu, L Hu, *Chinacrypt 94 pp 141–146 (in Chinese)*

This paper uses Gröbner basis theory to prove that windows of two dimensional linear recurring arrays of minimal degree must be trapezoidal. A simplified proof of the expression of irreducible arrays, using ideal extension theory, is provided and the periods of ideals are calculated.

034528 'An Enigma in the Classroom'

EK Lloyd, *Bulletin of the IMA v 30 no 9 (Sep/Oct 94) pp 156–158*

The author describes teaching undergraduates about the Enigma. One of his students found a flaw in the classical theory: the traditional analysis can occasionally be frustrated by a consistent but incorrect reflector wiring, such as where the effect is differently aligned 3-cycles in the same overall cycle structure.

034529 'Some results on the calculation of linearly independent latin squares'

Y Long, *Chinacrypt 94 pp 238–244 (in Chinese)*

This paper discusses arrays of linearly independent Latin squares, and produces some counting results for squares corresponding to linearly independent invertible vector Boolean functions.

034530 'An Ideal Method for Multisequence Synthesis'

PZ Lu, GW Song, JJ Zhou, *Chinacrypt 94 pp 193–200*

In this paper, the homogeneous ideal method for linear sequence synthesis is extended to solve the problem of multi-sequence synthesis. The authors obtain a constructive algorithm for calculating the generators of the characteristic homogeneous ideal for the synthesis.

034531 'A Fourier Transform Approach to the Linear Complexity of Nonlinearly Filtered Sequences'

JL Massey, S Serconek, *Crypto 94 pp 332–340*

The authors provide a new technique for analysing the linear complexity of nonlinearly filtered m-sequences. This uses discrete Fourier transform techniques, and rests on Blahut's theorem that that the linear complexity of an n-periodic sequence in $GF(q^n)$ is equal to the Hamming weight of its frequency domain associate. They generalise a result of Key by showing that a second order product of two distinct phases of an m-sequence never degenerates provided only that the degree of its minimal polynomial is prime.

034532 'The First Experimental Cryptanalysis of the Data Encryption Standard'
M Matsui, *Crypto 94 pp 1–11*

The author describes the first experimental attack on DES using 12 workstations in fifty days to analyse a corpus of 2^{43} known plaintext-ciphertext pairs. Generating these pairs and incrementing 2^{13} counters took forty days; the remaining ten days were spent on searching 2^{39} candidate keys. The attack was based on two 14-round linear approximations to DES, which hold with probability about 2^{-21} different from 0.5.

034533 'A Sublinear Algorithm for Approximate Keyword Searching'
EW Myers, *Algorithmica v 12 no 4/5 (Oct/Nov 94) pp 345–374*

The author provides an algorithm which finds approximate matches between a short subject string and a long target string (that is, matches subject to a bounded number of insertions, deletions and mismatches) in time sublinear in the length of the target string.

034534 'An Analysis of a Class of Algorithms for S-box Construction'
L O'Connor, *Journal of Cryptology v 7 no 3 (summer 94) pp 133–151*

The author examines a previously proposed method for constructing S-boxes one bit at a time so that they satisfied various avalanche and nonlinearity criteria, and shows that it is not feasible for more than 8 inputs. In particular, constructing an m-bit permutation a bit at a time using a greedy algorithm costs $O(e^{m^2})$.

034535 'Algebraic Nonlinearity and Its Application to Cryptography'
L O'Connor, A Klapper, *Journal of Cryptology v 7 no 4 (autumn 94) pp 213–227*

The authors give a probabilistic analysis of algebraic nonlinearity. The average degree of the polynomial which represents an n-bit Boolean function is $n + o(1)$, and if it is balanced, then any subfunction resulting from holding less then $n - \lceil \log n \rceil - 1$ bits constant is likely to be nonaffine. The number of Boolean functions with a linear structure is also counted.

034536 'Fast Cryptanalysis of the Fast Data Encipherment Algorithm'
K Ohta, K Aoki, *Crypto 94 pp 12–16*

The authors searched for 5-round and 7-round linear approximations to FEAL, and concluded that 8-round FEAL can be attacked using 2^{26} known plaintexts for sure, and using 2^{25} known plaintexts with probability 70%.

034537 'Cryptographic hash functions'
B Preneel, *European Transactions on Telecommunications v 5 no 4 (Jul/Aug 94) pp 431–448*

The author discusses the history of cryptographic hash functions and their applications in cryptology. Then he reviews the information theoretic, complexity theoretic, and practical approaches to constructing them. The most important practical constructions are listed, together with attacks on them, and an overview is given of standardisation in this area.

034538 'Structural analysis of product sequence families over the ring $Z/(p^d)$'
WF Qi, JJ Zhou, *Chinacrypt 94 pp 173–179 (in Chinese)*

This paper describes the structure of the product $G(f_1(x))G(f_2(x)) \cdots G(f_k(x))$, where $f_i(x)$ is a monic strong non-multiple polynomial over $Z/(p^d)$ and $G(f_i(x))$ is the set of all linear recurring sequences over $Z/(p^d)$ with characteristic polynomial $f_i(x)$. It gives conditions on the monic polynomial $h(x)$ such that $G(f_1(x))G(f_2(x)) = G(h(x))$ exists, and the conditions on the monic polynomials $h_1(x), h_2(x), \ldots, h_k(x)$ such that $G(f_1(x))G(f_2(x)) \ldots G(f_k(x)) = G(h_1(x)) + G(h_2(x)) + \cdots + G(h_k(x))$ exists.

034539 'The RC5 Encryption Algorithm'

RL Rivest, *Dr Dobbs Journal no 226 (Jan 95) pp 146–148*

The author describes his latest block cipher, RC5, which uses data dependent rotations and can be parametrised for varying key lengths and for different word and key sizes.

034540 'The GOST Encryption Algorithm'

B Schneier, *Dr Dobbs Journal no 226 (Jan 95) pp 123–124*

The author describes the Russian GOST 28147-89 algorithm - the Soviet equivalent of DES. Like DES, it is a Feistel cipher, but it has a simpler round function and twice as many rounds.

034541 'Pitfalls in Designing Substitution Boxes'

J Seberry, XM Zhang, YL Zheng, *Crypto 94 pp 383–396*

The authors prove that many types of S-box which might be desirable do not exist. For example, for $n > 4$, there is no quadratic n by s uniformly half-occupied box if n or s is even; and we can neither add not subtract components from a uniformly half-occupied box without losing this property.

034542 'An Introduction to Cryptanalysis'

KA Siil, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 24–29*

The author explains basic cryptanalytic techniques with reference to monoalphabetic substitution ciphers.

034543 'Encryption and decryption algorithms of heat flow cryptosystems in the non-homogeneous linear and semi-linear cases'

HY Song, ZF Chu, DH Li, *Chinacrypt 94 pp 33–40 (in Chinese)*

This paper discusses the non-homogeneous linear case and semi-linear case of heat flow cryptosystems. The algorithms for encryption and decryption were given in form of mixed problems of which the solutions are unique for the non-homogeneous linear and semi-linear pseudo-parabolic partial differential equations. Differences schemes with second order accuracy were established for the numerical solutions of these algorithms. A software implementation of these algorithms was introduced.

034544 'On the Existence of Cyclic Hadamard Difference Sets'

HY Song, SW Golomb, *IEEE Transactions on Information Theory v 40 no 4 (July 94) pp 1266–1268*

Balanced binary sequences with two-level autocorrelation are known to be related to cyclic Hadamard difference sets. The authors conjecture that the length of such sequences must be a prime, a product of twin primes, or one less than a power of two. This has been checked for all sequence lengths up to 1,000, and up to 10,000 with at most 17 exceptions.

034545 'Hashing with SL_2'

JP Tillich, G Zémor, *Crypto 94 pp 40–49*

The authors propose a new family of hash functions based on special linear groups over fields of characteristic two. The difficulty of finding collisions can be reduced to group-theoretic problems, and any local modification of the text which did not change the hashcode would constrain the girth of the associated Cayley graph.

034546 'Ciphertext Only Attack for One-way function of the MAP using One Ciphertext'

Y Tsunoo, E Okamoto, T Uyematsu, *Crypto 94 pp 369–382*

MAP is a hash function primitive based on 4-round FEAL with feedforward. It is shown to be very weak, in given a single 64-bit ciphertext we can recover the corresponding plaintext in only $O(2^{32})$ computations; this was demonstrated in 15.7 hours on a SPARCstation 2. The attack comes about in part because the FEAL round function has an inverse.

034547 'On Distribution of Boolean Functions with Nonlinearity $\leq 2^{n-2}$'

CK Wu, *Chinacrypt'94 pp 265–272*

The author studies the distribution of Boolean functions of n variables with nonlinearity $\leq 2^{n-2}$ by considering the cosets of the affine functions. The number of cosets depends on whether any of them contains more than one function of minimum Hamming weight 2^{n-2}.

034548 'Some Results on Multiples and Numerical Multiplier Groups of Difference Sets'

Q Xiang, *Graphs and Combinatorics v 10 no 3 (94) pp 293–304*

The difference sets in arbitrary finite groups can be studied by means of their characters and multipliers. A number of results are proved, including certain properties of skew Hadamard difference sets in Abelian groups.

034549 'On the non-linearity measure and construction of permutations'

GZ Xiao, DG Feng, *Chinacrypt 94 pp 252–256 (in Chinese)*

This paper describes a new way for measuring non-linearity of permutations — kth order non-linearity. It gives a spectral representation of kth order non-linearity of permutations and discusses some methods for constructing permutations of high kth order non-linearity.

034550 'On the construction of large S-boxes'

JH Yang, KC Zeng, QB Di, *Chinacrypt 94 pp 24–32 (in Chinese)*

Theoretical analysis and statistical data shown that large S-boxes are more secure than smaller ones. However, large S-boxes are also more difficult to design and to implement. This paper describes a method for constructing large (n, n) S-boxes based on conjugate classes of the finite field $GF(2^n)$ under normal bases. It also describes some methods for computing the cryptographic parameters of these S-boxes. This construction method greatly simplifies the design and software implementation of large S-boxes.

034551 'A Modified Design Criterion For Stream Ciphers'

M Zhang, G Xiao, *Chinacrypt 94 pp 201–209*

Linear complexity, correlation immunity, and linear consistency are three important design criteria for stream ciphers. In this paper, the connections between them are summarised and the correlation immunity criterion is criticised for being impractically severe. A modified criterion — ϵ-correlation immunity — is proposed: essentially, this means that the correlation is bounded by ϵ. It turns out that this can be characterised in terms of Walsh transforms. Finally, a class of Boolean functions is introduced, the nonrepetitive kth order forms, which have the same asymptotic spectral properties as bent functions.

034552 'A fast algorithm for the generation of k-ary De Bruijn sequences'

SX Zhu, *Chinacrypt 94 pp 135–140 (in Chinese)*

This paper presents a new algorithm for the generation of k-ary de Bruijn Sequences by juxtaposing periodic reductions of sequences of lower order. The algorithm is claimed to reduce the time taken to generate these sequences.

6 Public Key Algorithms

034601 'Interleaving security and efficiency considerations in the design of inexpensive IC cards'
B Arazi, *IEE Proceedings on Computers and Digital Techniques v 141 no 5 (Sep 94) pp 265–270*

A new kind of public key scheme is proposed in which the secret key is buried in a complex hash function built up from multiplexers; its security depends on the composition of nonlinear Boolean functions being hard to factor. Its claimed advantage over existing algorithm types is that it could be implemented directly in smartcard chips to support a low cost challenge-response protocol.

034602 'Incremental Cryptography: The Case of Hashing and Signing'
M Bellare, O Goldreich, S Goldwasser, *Crypto 94 pp 216–233*

The authors consider how one might construct signature schemes so that an update of a message could be signed quickly. Various algorithms are discussed; for example one can have a series of generators g_1, g_2, ... of a group and hash the message $M_1 M_2$... as $g_1^{M_1} g_2^{M_2}$..., and signatures can be constructed similarly.

034603 'Cryptographic Protocols Based on Discrete Logarithms in Real-quadratic Orders'
I Biehl, J Buchmann, C Thiel, *Crypto 94 pp 56–60*

The authors present a variant of the ElGamal signature scheme based on an 'exponentiation' function defined on the set of reduced principal ideals of a real quadratic order. This function has the property that a general algorithm for inverting it could also be used to factor integers.

034604 'On the Risk of Opening Distributed Keys'
M Burmester, *Crypto 94 pp 308–317*

A number of Diffie-Hellman type systems can be broken if a used session key is leaked or lost, including schemes proposed by Goss, Günther, Yacobi and the European Commission's RIPE project. The essential weakness of these schemes is to use only one instance of the Diffie-Hellman problem to generate multiple session keys.

034605 'Array codes for private-key encryption'
RM Campello de Souza, J Campello de Souza, *Electronics Letters v 30 no 17 (18 Aug 94) pp 1394–1395*

The authors present a secret key block encryption algorithm which is based on the burst error correcting codes of Blaum, Farrell and Van Tilborg.

034606 'Some new MC knapsack cryptosystems'
ZF Cao, G Zhao, *Chinacrypt 94 pp 70–75 (in Chinese)*

This paper presents new knapsack cryptosystems — MCS2 and MCS3 — which are based on the matrix cover problem, and which resist the cryptanalytic techniques applied to integer knapsack schemes. Their key sizes are comparable to those proposed for the Merkle-Hellman scheme.

034607 'Exact Algorithms for the Setup Knapsack Problem'
ED Chajakis, M Guignard, *Information Systems and Operational Research v 32 no 3 (Aug 94) pp 124–142*

The authors provide a dynamic programming algorithm which solves a class of knapsack problems in at worst pseudopolynomial time.

034608 'Improved Girault Identification Scheme'
K Chen, *Electronics Letters v 30 no 19 (15 Sep 94) pp 1590–1591*

The author proposes making the Girault identification scheme more efficient by using rank distance codes.

034609 'Rank distance codes and their application in identification'
K Chen, *Chinacrypt 94 pp 93–99*

In this paper, the author generalises Gabidulin's idea of rank metric and rank distance codes and applies them to provide a zero-knowledge identification scheme which uses smaller keys than Stern's scheme.

034610 'A practical secret voting scheme which allows voters to abstain'
L Chen, M Burmester, *Chinacrypt 94 pp 100–107*

The paper proposes a practical secret voting scheme which is provably robust and verifiable, and can be based on blinded versions of Fiat-Shamir together with bulletin boards. A conspiracy of adversaries who disrupt or falsify the voting of the election will be detected with high probability. The privacy of the voters is unconditionally protected; voters may abstain from the election, and intermediate results of the voting do not leak.

034611 'Invariants and invertibility of linear finite automata'
ZD Dai, *Chinacrypt'94 pp 127–134 (in Chinese)*

This paper studies the action of transformation groups on linear finite automata. The weak invertibility of these automata are characterised in terms of group invariants, which also give the ranks of matrices produced by Tao's algorithms. Studying the equivalence classes shows that the number of reduced transfer functions is finite, and these classes can be parametrised in a way which facilitates the construction of transfer function matrices with known invariant factors.

034612 'In Identity-Based Signature Scheme with Bounded Life-Span'
O Delos, JJ Quisquater, *Crypto 94 pp 83–94*

By combining the Guillou-Quisquater scheme with a Lamport scheme, the authors produce a signature scheme which can be used to sign only a fixed number of messages. Whenever one of these signatures is verified, a record is kept in a public directory, so that the double use of a secret can be detected. Suggested applications include prepayment tokens.

034613 'Threshold cryptography'
YG Desmedt, *European Transactions on Telecommunications v 5 no 4 (Jul/Aug 94) pp 449–457*

This is an overview paper on threshold cryptosystems, where at least t members from a group of n are required to perform a cryptographic operation. The discussion is restricted to the case where there is only interaction with an untrusted server, and no internal interaction between the participants. The paper motivates the need for these systems, and gives examples for threshold decryption, threshold pseudorandom generators, threshold authentication and signatures, and threshold zero-knowledge proofs.

034614 'An Efficient Existentially Unforgeable Signature Scheme and Its Applications'
C Dwork, M Naor, *Crypto 94 pp 234–246*

An existentially unforgeable scheme is one in which an opponent can have a large number of chosen messages signed, but still cannot generate a valid signature on any other message. The authors present such a scheme, which combines ideas from RSA and tree authentication, and which takes about six times as much computation as RSA. A suggested application is securing computer based fax.

034615 'On quadratic residues and nonresidues in difference sets modulo n'
J Fabrykowski, *Proceedings of the AMS v 122 no 2 (Oct 94) pp 325–331*

The author investigates the maximum number of elements in a set whose members, and their pairwise differences, are all quadratic residues modulo n. In particular, if n is a prime congruent to 3 modulo 4, then this set is empty; but if n's prime divisors are all congruent to 1 modulo 4, then a lower bound on the cardinality of A can be given. There are also results for nonresidues.

034616 'A Fast Approximation Algorithm for the Subset-Sum Problem'
G Gens, E Levner, *Information Systems and Operational Research v 32 no 3 (Aug 94) pp 143–148*

The authors show how to improve on previous algorithms for obtaining approximate solutions for knapsack problems.

034617 'A Survey of Parallel Algorithms for One-Dimensional Integer Knapsack Problems'
TE Gerasch, PY Wang, *Information Systems and Operational Research v 32 no 3 (Aug 94) pp 163–186*

The authors consider how a number of knapsack problems might be tackled by a parallel processor; they review previous work and obtain some complexity bounds.

034618 'On the length of cryptographic hash-values used in identification schemes'
M Girault, J Stern, *Crypto 94 pp 202–215*

The authors investigate the length of the hash values used with a number of identification schemes, including Fiat-Shamir and Schnorr. A number of birthday attacks are possible, making 64-bit hash values quite insecure. Variants are presented which resist collision attacks and which also minimise the number of communicated bits for any given security level. Security typically depends on the opponent's being unable to find a multiple collision in the hash function, that is $h(M_1) = h(M_2) = ... = h(M_r)$ for some value of r.

034619 'An analysis of the finite automata public key algorithm'
H Guan, *Chinacrypt 94 pp 120–126*

The author presents a chosen ciphertext attack on the FAKPC2 public key cryptosystem, which works when the dimension is small enough. He then proposes a modification of the system to thwart it.

034620 'Group-oriented (t,n) threshold digital signature scheme and digital multisignature'
L Harn, *IEE Proceedings on Computers and Digital Techniques v 141 no 5 (Sep 94) pp 307–313*

The author presents a number of threshold signature schemes based on ElGamal, one of which does not require a mutually trusted dealer to set it up.

034621 'Design of generalised ElGamal type digital signature schemes based on discrete logarithm'
L Harn, Y Xu, *Electronics Letters v 30 no 24 (24 Nov 94) pp 2025–2026*

The authors present the first systematic analysis of which ElGamal-type digital signature schemes are possible. Where the secret key is x, the message key is k and $r = g^k$ for some generator g of a high-order subgroup of Z_p^*, the signature r, s is in general determined by $ax = bk + c$ where a, b and c are the public values r, s and the message m, or products of them. It turns out that there are eighteen combinations which work, and which include existing schemes such as ElGamal and Schnorr as examples. The computational costs and subliminal channel properties of such schemes are also discussed.

034622 'LUC public key cryptosystem and its properties'
DK He, *Chinacrypt 94 pp 60–69 (in Chinese)*

This paper describes the LUC public key cryptosystem, and classifies plaintexts according to their periods. It points out that pseudo-periods exist in the LUC system, and proposes criteria for selecting system parameters. It also proposes a new scheme which combines the ideas of LUC and RSA.

034623 'A Parallel Permutation Multiplier for a PGM Crypto-Chip'
T Horváth, SS Magliveras, TY Trung, *Crypto 94 pp 108–113*

The authors describe an experimental FPGA implementation of the second author's PGM cryptosystem. This uses a crossbar switching system to compose permutations, and acts as a coprocessor to a DSP chip.

034624 'Some Complexity Issues in a Class of Knapsack Problems: What Makes a Knapsack problem Hard?'
D Krass, SP Sethi, G Sarger, *Information Systems and Operational Research v 32 no 3 (Aug 94) pp 149–162*

The authors consider the difficulty of certain knapsack problems on a subset S of the positive integers. Varying S gives a range of difficulty: if S is the range of a suitable polynomial then the problem is NP-complete, while if it is the linear transform of a function satisfying $F(z+1) = (z+1)f(z)$ and $f(0) = 1$ then there is a polynomial time solution.

034625 'Security of RSA type cryptosystems over elliptic curves against Hastad attack'
H Kuwakado, K Koyama, *Electronics Letters v 30 no 22 (27 Oct 94) pp 1843–1844*

The Demytko and KMOV systems, which are elliptic curve variants of RSA, had been claimed to be resistant to low exponent attacks on linearly related plaintexts. This claim is shown to be excessive; for example, the Demytko system with public exponent 3 can be attacked with 49 related plaintexts. However, with exponent 5 or more and a modulus of 511 or more bits length, both these systems are secure against this kind of attack.

034626 'Conspiracy attacks on the threshold RSA signature scheme'
CM Li, TNL Hwang, NY Lee, *Cryptologia v XVIII no 4 (Oct 94) pp 372–380*

The authors make the trivial remark that if more than the threshold number of players conspire in the Desmedt-Frankel scheme, they can recover the shared secret.

034627 'An Extension of Low-Density Subset Sum Algorithm and Its Applications in Cryptanalysis'
DX Li, LR Lu, *Chinacrypt 94 pp 17–23*

The authors extend the subset sum problem by allowing variables to be in the range $\{-1, 1\}$. They prove that almost all extended subset sum problems of density $< 0.488\cdots$ can be solved in polynomial time. The application of this result to the cryptanalysis of the Idempotent Element cryptosystem is presented.

034628 'Cryptanalysis of extended linear code public-key cryptosystem'
DX Li, XY Wang, *Chinacrypt 94 pp 1–6 (in Chinese)*

This paper discusses the extended linear code public-key cryptosystem. This was invented by Shi Xiaoming in 1988 and is based on the difficulty of decoding an extended linear code. It presents a cryptanalysis of this cryptosystem which uses Euclid's Algorithm to find the pair of decryption keys.

034629 'Security of interactive DSA batch verification'
CH Lim, PJ Lee, *Electronics Letters v 30 no 19 (15 Sep 94) pp 1592–1593*

The authors break the batch DSA scheme of Naccache and others; either the signer or the verifier can easily generate a set of bogus signatures which satisfy the batch verification criterion, and if such bogus signatures are inserted into a system there is no way to tell which party was responsible.

034630 'Public Key Cryptography'
AM Odlyzko, *AT & T Technical Journal v 73 no 5 (Sep/Oct 94) pp 17–23*

The author provides a tutorial on public key techniques, including Diffie Hellman and RSA systems, and describes the IS-S4-B system used for key management in North American cellular phones.

034631 'Designated Confirmer Signatures and Public-Key Encryption are equivalent'
T Okamoto, *Crypto 94 pp 61–74*

The author formalises Chaum's idea of a designated confirmer signature, and proves that such signatures exist if and only if a public key cryptosystem does. This gives rise to a new practical construction for these signatures which are more efficient than previous systems.

034632 'Sequences in τ-quasi-linear finite automata and their application in cryptanalysis'
ZP Qin, HG Zhang, *Chinacrypt 94 pp 112–119 (in Chinese)*

This paper examines sequences in τ-quasi-linear finite automata and discusses the security of the identity-based and signature variants of the finite automata public key cryptosystem.

034633 'Factorizations in the Elementary Abelian p-Group and Their Cryptographic Significance'
MH Qu, SA Vanstone, *Journal of Cryptology v 7 no 4 (autumn 94) pp 201–212*

The authors break a knapsack based public key system proposed by Webb. Their attack is based on the factorisation properties of elementary Abelian p-groups.

034634 'Secure Voting Using Partially Compatible Homomorphisms'
K Sako, J Kilian, *Crypto 94 pp 411–424*

Previous schemes for electronic elections were either mixers, in which n centres in series shuffle the votes, or divide-vote schemes, in which there are n centres in parallel. Mixers are more efficient, while divide-vote schemes let anyone check that every vote was counted correctly. The present paper provides a much more efficient divide-vote scheme, with a data requirement of 56Kbyte per vote rather than the 4MByte of previously proposed systems.

034635 'A Key-Exchange Protocol Using real Quadratic Fields'
R Scheidler, JA Buchmann, HC Williams, *Journal of Cryptology v 7 no 3 (Summer 94) pp 171–199*

The authors develop the algorithms to do Diffie Hellman key exchange using the ideals of a real quadratic field. The technical details which are tackled include resolving ambiguities in the computation by looking at neighbouring ideals.

034636 'Solving subset sum systems and breaking pure fraction knapsack cryptosystems'
ZH Shao, *Chinacrypt 94 pp 7–16 (in Chinese)*

The author uses probabilistic methods to compute the expected number of short vectors in an integer lattice, and proves a conjecture presented by Lagarias and Odlyzko in 1985. He also modifies the L^3 lattice basis reduction algorithm to break the pure fraction knapsack cryptosystem.

034637 'Designing Identification Schemes with Keys of Short Size'
J Stern, *Crypto 94 pp 164–173*

In this paper, a new practical identification protocol is presented whose security relies on a non-arithmetic problem, the constrained linear equations problem. This consists of solving a system of linear modular equations whose unknowns are restricted to specific subsets of the integers. This scheme allows the use of short keys — comparable in length with those of symmetric key systems.

034638 'Construction of dynamic threshold schemes'
HM Sun, SP Shieh, *Electronics Letters v 30 no 24 (24 Nov 94) pp 2023–2025*

The authors provide an ElGamal-based threshold scheme in which a given number of shareholders can redistribute shares by recalculating a public function rather than by replacing their shares.

034639 'A note on finite automata public key cryptosystems'
R Tao, S Chen, *Chinacrypt'94 pp 76–81*

Finite automata public key cryptosystems provide both encryption and digital signatures. In this system, encryption is randomised in the sense that the ciphertext of any plaintext can be chosen from a large space; however, signature generation did not until now have this property. This paper discusses ways to randomise digital signatures and to reduce the size of the secret key.

034640 'An extension of the transition functions in finite automata public key cryptosystems'
H Wang, *Chinacrypt 94 pp 108-111 (in Chinese)*

In a given state, a finite automaton $M = (X, Y, S, \delta, \lambda)$ behaves as a transducer that, via its transition function δ and its output function λ, converts an input sequence to an output sequence. This paper suggests an extension of the transition function, and examines certain properties of the new δ. The succession property of the extended δ is used to prove theorems about initial, final, and synchronising state test sequences.

034641 'Analysis and improvement of an access control scheme with user authentication'
SM Yen, CS Laih, *IEE Proceedings on Computers and Digital Techniques v 141 no 5 (Sep 94) pp 271–273*

The authors show how a recently proposed authentication and access control scheme can be made more efficient and have a number of features added.

034642 'A note on RSA public-key system'
XY Yu, *Chinacrypt 94 pp 53–59 (in Chinese)*

The author considers the number of fixed points of the function $x^n (\mathrm{mod}\ m)$, and concludes that the more prime factors the modulus of the RSA cryptosystem contains, the weaker it may be - independently of the effect this may have on the time taken to factor it.

7 Computational Number Theory

034701 'Polynomial Algorithm for Linear Programming over the Algebraic Numbers'
I Adler, PA Beling, *Algorithmica v 12 no 6 (Dec 94) pp 436–457*

The authors generalise the ellipsoid method to solve linear programming problems over the algebraic numbers. One of the problem size parameters is the maximum degree of any algebraic number which can occur during the computation.

034702 'Sums Involving the Smallest Prime Factor of an Integer'
HZ Cao, *Utilitas Mathematica v XLV (1994) pp 245–251*

The author evaluates $\sum_{n \leq x} \phi(n)/p(n)$ and $\sum_{n \leq x} 1/(n \log p(n))$ where $p(n)$ is the smallest prime factor of n.

034703 'Design of Elliptic Curves with Controllable Lower Boundary of Extension Degree for Reduction Attacks'
JH Chao, K Tanada, S Tsujii, *Crypto 94 pp 50–55*

If an elliptic curve over $GF(q)$ has order m, and the smallest prime divisor of $\phi(m)/2$ is B, then using the Menezes-Okamoto-Vanstone technique to reduce the elliptic logarithm problem to discrete logarithm in an extension of $GF(q)$ will involve an extension degree of at least B. This result can be used with the Atkin-Morain construction to produce elliptic curves on which the reduction attack is unfeasible, and an example of such a curve is given.

034704 'On the accurate calculation of $\pi(10^9)$ and its proof data'
SL Cheng, ZQ Han, XL Wang, *Chinacrypt 94 pp 245–251 (in Chinese)*

The authors calculated the number of prime numbers smaller than 1,000,000,000 in 1992, and obtained the value 50847534. However, many writers on number theory and cryptography from Hardy and Wright onwards had quoted the value 50847478. In order to prove the correctness of their calculation, the authors discuss their software and report a number of tests and cross-checks.

034705 'Algorithm of polynomial complexity for factoring polynomials over local fields'
AL Chistov, *Journal of Mathematical Sciences v 70 no 4 (10 July 94) pp 1912–1933*

The author provides an algorithm for factoring multivariate polynomials over local fields. This is polynomial in the length of the input and the characteristic of the residue field.

034706 'Fast square-and-multiply exponentiation for RSA'
LCK Hui, KY Lam, *Electronics Letters v 30 no 17 (18 Aug 94) pp 1396–1397*

The authors provide a new method of performing modular exponentiations quickly. It can reduce the time taken to a linear function of the modulus size, but at the cost of an exponential increase in the number of precomputed values. However, even for modest amounts of precomputation, this algorithm can provide more speedup than many previously proposed approaches.

034707 'The Number of Steps in the Euclidean Algorithm'
D Hunsley, *Journal of Number Theory v 49 no 2 (Nov 94) pp 142–182*

The number of steps needed to calculate $\gcd(a, b)$ for $a < b$ had been known to be about $(12 \log 2/\pi^2) \log b$. The author proves that this is the mean number of steps, and that the variance is $C \log b$ for a certain constant C.

034708 'Factoring'
AK Lenstra, in *Distributed Algorithms, Springer LNCS v 857 (1994) pp 28–38*

The author surveys the progress of factoring since the 1970's and gives and overview of the continued fraction, quadratic sieve and number field sieve algorithms. He argues that future progress has been consistently underestimated and that 512-bit RSA keys are very close to being crackable.

034709 'More Flexible Exponentiation with Precomputation'
CH Lim, PJ Lee, *Crypto 94 pp 95–107*

The authors show that one can speed up the calculation of g^R by splitting R into two halves, $R = R_1 + 2^{n/2}R_2$, and precomputing $g^{2^{n/2}}$. They discuss how it can be parallelised and compare its performance with existing precomputation algorithms.

034710 'Towards the Equivalence of Breaking the Diffie-Hellman Protocol and Computing Discrete Logarithms'
UM Maurer, *Crypto 94 pp 271–281*

An oracle for the Diffie-Hellman problem — one which enables us to calculate g^{xy} from g^x and g^y — will also let us calculate functions such as g^{x^2}, $g^{1/x}$ and $g^{\sqrt{x}}$ provided that the order of the group is known. Thus we can find a y such that (g^x, g^y) is a point on a suitable elliptic curve, and the upshot is that if discrete logarithms on this curve are easy (as they will be if the order is smooth), then the Diffie-Hellman and discrete log problems are equivalent. In particular, this will be the case if every prime factor p of $|G|$ occurs only once, and has $p-1$ smooth; or if we can construct a smooth order elliptic curve over $GF(p)$.

034711 'Fast Generation of Provable Primes Using Search in Arithmetic Progressions'
P Mihailescu, *Crypto 94 pp 282–293*

The author examines the cost of finding provable primes in arithmetic progressions. He concludes that it is never more than 2% slower than probabilistic prime methods, and is actually more efficient for primes of less than 1000 bits length.

034712 'Primitive normal polynomials over finite fields'
IH Morgan, GL Mullen, *Mathematics of Computation v 63 no 208 (Oct 94) pp 759–765 and S19–S23*

The authors extend the tables of primitive normal polynomials by giving a minimal example for each $p^n < 10^{58}$ with $p \leq 97$. They conjecture that for all $n \geq 2$, there is a primitive normal polynomial of degree n with weight at most 4, and that for all $a \neq 0$ there is a primitive polynomial of degree n and trace a provided $n > 2$.

034713 'VLSI structures for bit-serial modular multiplication using basis conversion'
MG Parker, M Benaissa, *IEE Proceedings on Computers and Digital Techniques v 141 no 6 (Nov 94) pp 381–390*

The authors present a fast modular multiplier inspired by the Fourier transform over a finite field. Their design uses two redundant representations to get a high throughput bit serial process, where much of the complexity is transferred to basis conversion operations which can be done systolically.

034714 'Two Fast Parallel Prime Number Sieves'
J Sorenson, I Parbury, *Information and Computation v 114 no 1 (Oct 94) pp 115–130*

The authors propose and analyse parallel versions of the sieve of Eratosthenes: one runs in $\mathrm{O}(\log n)$ time on $\mathrm{O}(n/(\log n \log\log n))$ processors, while the other runs in $\mathrm{O}(\sqrt{n})$ time on $\mathrm{O}(\sqrt{n})$ processors.

034715 'Logarithmic speed modular multiplication'
CD Walter, *Electronics Letters v 30 no 17 (18 Aug 94) pp 1397–1398*

Most special devices for doing fast modular multiplication of n-bit integers take $O(n \log n)$ time and $O(n)$ space using redundant number systems to limit carry propagation. However, it is possible to achieve $O(\log n)$ time at the cost of $O(n^2)$ space by using fast (Wallace tree) circuits for the underlying integer multiplication step. This means that, for example, a 50-fold increase in speed can be bought for 500 bit RSA at the cost of a 400-fold increase in chip area.

034716 'The window method for computing exponentiation'

J Ye, *Chinacrypt 94 pp 210-213 (in Chinese)*

This paper describes a fast exponentiation method: the window method. It is a variant of the addition chain method and is easy to implement.

034717 'The generalisation of Gröbner bases theory and a synthesis algorithm of two-dimensional arrays over the ring $Z/(m)$'

JJ Zhou, YJ Zhou, ZF Wang, *Chinacrypt 94 pp 161-172 (in Chinese)*

This paper generalises Sakata's results on Gröbner basis theory to certain $Z/(p^e)$-algebras whose rings are Noetherian. This yields a new synthesis algorithm for two dimensional arrays over $Z/(m)$, whose complexity is $O(n^2)$.

034718 'Two problems of elliptic curves'

YJ Zhou, *Chinacrypt 94 pp 225-231 (in Chinese)*

This paper tackles two problems arising from elliptic curve cryptosystems. Firstly, for any elliptic curve over a finite field F_q, what is the probability that a given prime r divides the number of F_q-points of this elliptic curve? Secondly, for any given elliptic curve E over the rational numbers, let $\tilde{E}(F_p)$ be an elliptic curve reduced by E over a finite field F_p (for some prime p), does there exist a prime p such that a given prime r divides the number of F_q-points of $\tilde{E}(F_p)$? The author shows that infinitely many such primes exist.

8 Theoretical Cryptology

034801 'Directed Acyclic Graphs, One-Way Functions and Digital Signatures'
D Bleichenbacher, UM Maurer, *Crypto 94 pp 75–82*

Lamport's scheme for building signatures out of one-way functions is generalised to any directed acyclic graph, and this leads to a number of combinatorial questions. For example, when the vertex fan-in is at most two, we can find graphs which sign about half a bit per vertex.

034802 'Multi-Secret Sharing Schemes'
C Blundo, A De Santis, G Di Crescenzo, AG Gaggia, U Vaccaro, *Crypto 94 pp 150–163*

The authors prove information theoretic bounds on the size of shares which a set of participants must have in order to share a fixed number of secrets, and provide protocols for sharing two or three secrets which are optimal.

034803 'Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols'
R Cramer, I Damgård, B Schoenmakers, *Crypto 94 pp 174–187*

This paper combines two cryptographic systems, a proof of knowledge and a secret sharing system. If certain assumptions are made for these, then the proof can be transformed into a witness indistinguishable protocol in which the prover demonstrates knowledge of a certain relation associated with the secret sharing scheme.

034804 'Homomorphic Zero-Knowledge Threshold Schemes over Any Finite Abelian Group'
YG Desmedt, Y Frankel, *SIAM Journal of Discrete Mathematics v 7 no 4 (Nov 94) pp 667–682*

The authors introduce the concept of zero-knowledge threshold schemes to cover situations where the security of the distribution is computational rather than information theoretic, and thus extend the notion of a perfect secret sharing scheme. They then generalise their threshold scheme to arbitrary Abelian groups and arbitrary access structures.

034805 'Asynchronous Secure Computations with Optimal Resilience'
D Dolev, B Kelmer, T Rubin, *PDC 94 pp 183–192*

Previously, it had been known that secure multiparty computation in a fully connected network of n nodes could be carried out in the presence of up to $n/4$ Byzantine faults. The authors improve this to $n/3$, which they show to be the best possible.

034806 'Complexity Aspects of Guessing Prefix Codes'
AS Fraenkel, ST Klein, *Algorithmica v 12 no 4/5 (Oct/Nov 94) pp 409–419*

One can encipher text by adding a secret prefix and then doing Huffman coding. Attacks on such systems can be made harder by inserting a string of random bits after each occurrence of one or more plaintext strings. The problem of decrypting the resulting ciphertext is called 'subsequence prefix code' and is shown to be NP-complete, as are two similar problems. The authors suggest that these techniques might be used to combine compression and encryption for large databases on CD-ROM.

034807 'Reliable Broadcasting'
L Gargano, AL Liestman, JG Peters, D Richards, *Discrete Applied Mathematics v 53 (1994) pp 135–148*

Reliable broadcast can be guaranteed in a network with a bounded number of errors by introducing redundancy. The authors define k-reliable broadcasting and show that it requires $(k+1)n-(k+1)$ calls on an n-vertex graph.

034808 'Multistage secret sharing based on one-way function'
J He, E Dawson, *Electronics Letters v 30 no 19 (15 Sep 94) pp 1591–1592*

The authors present a secret sharing scheme in which each player uses the same shadow to reconstruct a number of secrets. These are reconstructed in stages from a number of public values published by the dealer. The cost is that for k secrets shared among n participants, there are kn public messages.

034809 'Language Independent Secure Bit Commitment'
T Itoh, Y Ohta, H Shiyuza, *Crypto 94 pp 188–201*

Two classes of languages are introduced, OT and TO. For any $L \in \mathrm{OT}$ there is a bit commitment function $f(x, b, r)$ (where b is a bit and x is an additional input) such that the distributions of $f(x, 0, r)$ and $f(x, 1, r)$ are identical if $x \in L$ and 'completely different' otherwise. For TO we have co-TO = OT. It is shown that if $L \in \mathrm{OT}$, then there is a perfect prover-practical zero-knowledge proof of L, and if $L\ in$ TO then there is a perfect bounded-round zero-knowledge proof for L.

034810 'New Bound on Authentication Code with Arbitration'
K Kurosawa, *Crypto 94 pp 140–149*

The author improves Johannson's bound on the size of the encoding rules needed for authentication with arbitration, especially when the size of the source state is large, and proposes a construction which approximately meets it.

034811 'A Randomness-Rounds Tradeoff in Private Computation'
E Kushilevitz, A Rosén, *Crypto 94 pp 397–410*

The authors demonstrate the effect of an extra random bit on the number of rounds needed for a private distributed computation: with 2 or more random bits, only $\Omega(\log n/d)$ rounds are necessary, and $O(\log n/\log d)$ are sufficient.

034812 'Construction of SM array codes for $d = 2$'
BG Lin, *Chinacrypt 94 pp 155–160 (in Chinese)*

This paper presents systems of SM array codes for $d = 2$, discusses the model and general properties of these codes, and gives construction principles and an example.

034813 'The optimal information rate of trees in secret sharing schemes'
XA Liu, *Chinacrypt 94 pp 87–92 (in Chinese)*

Blundo and others proved that the optimal information rate of secret sharing systems whose access structures are graphs is 1 or $\leq 2/3$. This paper shows that if the graph is a tree, then this rate cannot lie in the real interval $(3/5, 2/3)$, and gives necessary and sufficient conditions for it to be exactly 2/3. It also derives a lower bound on the optimal rate in terms of the order of the tree.

034814 'Computing Boolean Functions on Anonymous Networks'
E Kranakis, D Krizanc, *Information and Computation v 114 no 2 (Nov 94) pp 214–236*

The authors provide an algorithm for computing an arbitrary Boolean function on an anonymous network of m nodes, diameter d and maximal node degree n, which runs in time $\mathrm{O}(dn^3m^3 \log m)$, improving on the previous best of $\mathrm{O}(n^{m^2})$. Symmetric functions can be computed even more quickly.

034815 'Some applications of source coding in cryptography'
JL Massey, *European Transactions on Telecommunications v 5 no 4 (Jul/Aug 94) pp 421–429*

The author reviews five lossless source coding schemes and discusses the application of three universal schemes (Lynch-Davisson coding, Elias-Willems coding, and Lempel-Ziv coding) to cryptography: creating a strongly-ideal cipher, homophonic coding, testing random bit generators, and strengthening running key generators.

034816 'Computing roots of graphs is hard'
R Motwani, M Sudan, *Discrete Applied Mathematics v 54 no 1 (26/9/94) pp 81–88*

The authors show that the problem of deciding whether a graph (and equivalently a Boolean matrix) is a perfect square is NP-complete by reduction to NAESAT.

034817 'Hardness vs Randomness'
N Nisan, A Wigderson, *Journal of Computer and Systems Sciences v 49 no 2 (Oct 94) pp 149–167*

This is the journal version of the authors' FOCS 1988 paper proving that an arbitrary function which is hard for a given complexity class can be used to construct a bit generator whose output cannot be distinguished from a random sequence by any algorithm from that class.

034818 'On Constructing Secret Sharing Schemes'
SP Shieh, HM Sun, *IEEE Infocom 94 pp 1288–1292*

The authors propose a construction for secret sharing schemes with graph based access structures, which improves on a previous construction of Ho, Saito and Nishizeki.

034819 'Bounds on the Probability of Deception in Multiple Authentication'
B Smeets, *IEEE Transactions on Information Theory v 40 no 4 (July 94) pp 1586–1591*

One can integrate freshness into authentication schemes by changing the encoding rules between transmissions. In this case, the impersonation bound still holds, and the substitution bound is strengthened.

034820 'Functional Inversion and Communication Complexity'
SH Teng, *Journal of Cryptology v 7 no 3 (Summer 94) pp 153–170*

If a function of n variables can be computed by a multiparty computation protocol whose complexity is bounded by ϕ, then its inverse can be computed in $2^{O(\phi)}n$ steps. This gives an $\Omega(n \log n)$ bound on the area required to lay out any one-way function, and shows that some one-way functions cannot be computed with low communication complexity in certain topologies.

034821 'Constructing Cartesian authentication codes using pseudosymplectic geometry'
ZX Wan, RQ Feng, *Chinacrypt 94 pp 82–86 (in Chinese)*

This paper discussed the isomorphism problem of authentication codes. Two Cartesian authentication codes constructed from pseudo-symplectic geometry and the calculation of their parameters were given. In the case when the encoding rules are chosen according to a uniform probability distribution, the authors give the probabilities of a successful impersonation attack and a successful substitution attack. Finally, they prove the conditions under which these two authentication codes are isomorphic.

9 Book Reviews

'FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER'
William R Cheswick and Steven M Bellovin
Addison-Wesley, 1994; ISBN: 0-201-63357-4

The authors are researchers working for the AT&T Bell Laboratories. Over a number of years they have gathered information on accidental and deliberate breaches of the security of their employer's systems, and at other sites. This book is one of the most complete collections of anecdotes and advice on how to secure computers against attacks across a computer network; it should be required reading for computer network administrators and anybody else interested in practical computer security.

For each attack they suggest potential solutions and their possible consequences, allowing administrators to make informed choices as to the most suitable solution for their sites. The appendices provide a condensed version of this information for the administrator in a hurry. Appendix A describes useful security software and lists sites where this is available.

The bibliography is a model example which we hope others will follow. Where documents are available on-line you are told how to retrieve them. The authors have added a short abstract for those references where it would be helpful to the reader. Every reference is followed by a list of those pages on which it is referenced so that the reader can see the reference in context.

'COMPUTER RELATED RISKS
Peter G Neumann
Addison Wesley, 1995: ISBN 0-201-55805-X

For years now, Peter Neumann's newsgroup comp.risks has been the main single source of up to date information on real–world computer security breaches and on things which go wrong with automation generally. Now, in this book, he has collected together hundreds of the last decade's juiciest tales of electronic woe.

Many of these concern safety and reliability, especially in fields like medical and avionic systems, but a substantial number are security related. We read of a number of frauds against ATMs and other financial systems, viruses and other malicious code, flaws in password mechanisms (including Thompson's famous C-compiler Trojan horse), various other software trapdoors, cellular telephone and other telecom fraud, sabotage against corporate computer systems, bogus lottery tickets, election fraud, computer-assisted jailbreaks, and a whole host of privacy violations and mistaken identity cases.

This book is not just fun; it will be invaluable as a source of references, both as motivation for designers and for talks on computer security topics.

'FUNDAMENTALS OF COMPUTER SECURITY TECHNOLOGY'
Edward Amoroso
Prentice Hall, 1994; ISBN 0-13-10829-3

There has for some time been a need for a textbook which covers the issues tackled by researchers in operating systems and database security. Such a book has at last been produced by Ed Amoroso.

He works systematically through the topics covered at a typical conference in this field, starting from basic threat analysis and elementary attacks through security policies, classifications and clearances, the lattice model, Bell-LaPadula, nondeducibility, noninterference, the Biba and Clark-Wilson models, intrusion detection, covert channels, composability, kernels and database issues. This is not an exhaustive list, but serves to show how many topics are tackled which previously a graduate student could only learn from the research literature and at that with some difficulty.

The author states that his goal is to capture the state of the art in computer security, and it may be fairly said that this goal has been achieved. The style is readable, there are many examples taken from real systems, and there is a large annotated bibliography of many important research papers in the field. This book should be highly recommended as a textbook for the beginning graduate student, and in this context it will make the teacher's task much simpler.

'SECURITY-ANALYSIS OF A CLASS OF CRYPTOSYSTEMS BASED ON ERROR-CORRECTING CODES'
Johan van Tilburg
PhD Thesis, PTT Research. Leidschendam

Johan van Tilburg's thesis covers public key cryptosystems based on coding theory, and starts off with descriptions of the best known such systems — those of McEliece, Niederreiter and Stern. He proceeds to an extensive discussion of known security results, and describes a number of schemes which have been broken.

There follows a survey of decoding methods for general linear codes. A number of information set techniques are described, and these are shown to be equivalent to the permutation techniques which the author introduced in 1988. These are also related to syndrome decoding, for which a number of algorithms are developed and analysed. Next, majority voting techniques are used to tackle the Jordan-Rao scheme; and finally, the Rao-Nam and Li-Wang schemes are attacked by finding equivalent encoding schemes. This shows that these schemes need keys as large as McEliece for an equivalent level of security, contrary to their proposers' claims.

This book assumes a graduate mathematical background, and so would not be suitable as a textbook. However for the practitioner it is a good reference on this type of cryptosystem — and indeed the only one of which this reviewer is aware.

'A SHORT COURSE IN COMPUTER VIRUSES - SECOND EDITION'
Frederick B Cohen
Wiley 1994 ISBN 0-471-00769-2

Fred Cohen is uniquely qualified to write about computer viruses, having invented them twelve years ago as his PhD project. In addition to a brief history of the subject, this new version of his book provides the up-to-date account of developments in the field; it is scientific rather than practical in that it discusses principles and advances in research rather than giving a blow-by-blow account of particular species.

Recent work covered includes that on the effect of network topology on virus propagation, as well as formal models of polymorphism - dealt with by treating viruses as families of programs - and the effect of trusted system defences. There is also a discussion of practical protection strategies and the relative value of tools such as integrity shells, snapshots and disk encryption, and a discussion of new viruses such as Cruncher which get past most scanners.

'CRYPTOLOGIE CONTEMPORAINE'
Gilles Brassard
Masson, 1993; ISBN 2-225-83970-0 (in French)

There is a shortage of good security books in languages other than English, and this is not just a nuisance for students; it can often be hard for engineers to find agreed translations of technical terms. For example, should one describe zero-knowledge proof in French as '*preuve zéro-connaissance*' or '*preuve à divulgation nulle*'?

These problems have now been solved for French speakers, and for people selling products and services to Francophone countries, by the appearance of this book. It is a French translation of the author's book 'Contemporary Cryptology', but it has been thoroughly revised and updated by him.

It does more, however, than just tell us to translate bit commitment as '*mise en gage*'. This is a thorough exposition, which covers not just the traditional ground of Shannon's results, DES and the basic public key techniques, but also recent developments such as differential cryptanalysis and the digital cash machinery. It closes with a *tour de force* - a detailed exposition of quantum cryptography, and a description of the technique's first successful implementation in 1991.

'FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY — LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES
Michael S Baum
U.S. Department of Commerce report number NIST-GCR-94-654

This book provides an extensive survey of the legal issues involved in the use of certificate-based public- key cryptography. It draws together information from a wide range of sources, including interviews with government officials and many documents that are not generally available. The main text is supported by numerous footnotes that give the relevant legal precedents.

The focus of the book is on the civil liability of a certification authority if anything goes wrong. It examines existing areas of law where the parties' potential liabilities are defined and understood, and identifies arguments that could be used to extend them to public-key cryptography. Areas which are described in detail include sovereign immunity and the Federal Tort Claims Act; the special status of common carriers; the special status of the U.S. Postal Service; and maritime shipping law.

The conclusions of the book are that the U.S. federal government should proceed with its plans to provide a Federal Certification Authority service; that the Federal Certification Authority should permit itself to be sued, although with limitations on its liability; that new legislation is needed to define the liability of a certification authority; and that in the absence of such legislation the terms of the contracts between a certification authority and its clients may be used to restrict liability.

By necessity, a work of this kind must be specific to one country's legal system. Although the general principles explained in this book are universally applicable, many of the details of points of law are only valid for the United States. Despite this, 'Federal Certification Authority Liability and Policy' is essential reading for everyone doing work in this field.

'WHO OWNS INFORMATION?'
Anne S Branscombe
Harper Collins 1994 ISBN 0-465-09175-X

Computer security professionals are increasingly coming up against privacy and data protection problems in addition to the more traditional requirements of organisational secrecy and transaction authenticity. The legal and political foundations of this subject are thus of potential importance, and these are Anne Branscombe's speciality.

In this book, she discusses the ownership of many different types of information - such as phone numbers, medical records, software copyright - from the point of view of US law. However, this is far from a dry legal textbook; it contains numerous case histories which are discussed in a lively way and which provides unusually broad insight into the essential problems of this subject.

'NETWORK SECURITY SECRETS
David J Stang, S Moon
IDG Books, 1994; ISBN 1-56884-021-7

This large and cheerful book is aimed at providing practical security know-how to computing people who are otherwise ignorant of the subject. It goes for breadth rather than depth; there are short chapters on a vast number of topics and products. For example, no less than twenty PC access control systems are evaluated, and there is considerable material on network systems such as LAN Manager, Netware and VINES, as well as on viruses.

With over 1100 pages, it is not light reading; but it does contain an eclectic variety of material which might always come in useful. It also comes with a large quantity of shareware which we did not examine, and with extensive appendices of vendor contacts, security conferences and the like.

How to Subscribe

Subscription orders are accepted for complete volumes only, starting with the first issue of any year. Continuing orders can also be made, and cancellations are accepted prior to the first issue of the year to which they apply. Claims for replacement of issues lost or damaged in the post should be made within six months. Subscribers may receive a complimentary electronic version of the journal by notifying us of their Internet email address.

Subscription rates: Corporate subscriptions cost £95, and individual subscriptions are available at the reduced rate of £60. Purchase orders are accepted for corporate subscriptions only. US Dollar cheques are accepted at an exchange rate of US$1.50 = £1; credit card orders (VISA and MasterCard) are charged in sterling.

Back issues offer: Get a subscription for 1995 (volume 4) plus a complete set of 1993 and 1994 back numbers (volumes 2 and 3) at a price of £90 for individual subscribers and £145 for corporate subscribers. This back number offer is only available while stocks last. Sorry, volume 1 is completely sold out!

Individual subscription for 1995 - Please debit my VISA/MasterCard £60 □ I enclose a cheque for £60 □ / US$90 □

Individual subscription for all 1993, 1994 and 1995 issues - Please debit my VISA/MasterCard £90 □ I enclose a cheque for £90 □ / US$135 □

Corporate subscription for 1995 - Please debit my VISA/MasterCard £95 □ I enclose a purchase order / cheque for £95 □ / US$142.50 □

Corporate subscription for all 1993, 1994 and 1995 issues - Please debit my VISA/MasterCard £145 □ I enclose a purchase order / cheque for £145 □ / US$212.50 □

Name: ....

Card number: ....Expiry Date: ....

Cardholder Address: ....

....

....

Delivery address (if different) ....

....

....

Email address: ....

Signature: ....

You can fax this order form to us on +44 223 334678, or mail it to us at:
Northgate Consultants Ltd., Ivy Dene, Lode Fen, Cambridgeshire CB5 9HF, United Kingdom