Computer and Communications

Security Reviews

Volume 4 Number 3 (September 1995) 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.

'Computer and Communications Security Reviews' is published quarterly by, and is copyright, of Northgate Consultants Ltd, whose registered office is Ivy Dene, Lode Fen, Lode, Cambridgeshire, United Kingdom CB5 9HF. Subscription rates, conditions and ordering details are on the inside back cover.

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by September 1995; 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:

CompCon95: Fortieth IEEE Computer Society International Conference, 5–9 March 1995, San Francisco, California; *proceedings published by the IEEE, ISBN0-8186-7029-0*

Oakland 95: 1995 IEEE Symposium on Security and Privacy, 8–10 May 1995, Oakland, California; *proceedings published by the IEEE, ISBN 0-8186-7015-0*

SAC 95: Workshop on Selected Areas in Cryptography, 18–19 May 1995, Ottawa, Canada; *workshop record published by School of Computer Science, Carleton University*

Eurocrypt 95: Held at St Malo, France, May 95; *proceedings published as Springer LNCS v 921*

CSFW 95: 8th IEEE Computer Security Foundations Workshop, 13–15 June 1995, Kenmare, Co. Kerry, Ireland; *proceedings published by the IEEE, ISBN 0-9186-7033-9*

NSIP 95: IEEE Workshop on Nonlinear Signal and Image Processing. 20–22 June 1995, Neos Marmaras, Halkidiki, Greece; *proceedings published by the IEEE*

CPAC 95: Cryptography — Policy and Algorithms Conference, 1–3 July 1995, Brisbane, Australia; *preproceedings published by Queensland University of Technology; full proceedings to be published by Springer*

IPR 95: International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, August 21–25, 1995; *proceedings published by Oldenbourg, Vienna, ISBN 3-7029-0408-5*

We have decided to place postscript versions of this journal in the public domain one year after publication. The goal is to strike a balance between providing a universal service and maintaining enough revenue to cover the costs of publication. Subscribers get paper copies, full latex source code for each issue, and a PGP key which enables them to download and decrypt the source code of all back numbers. The archives can be found at

`ftp.cl.cam.ac.uk/users/rja14`

or

`http://www.cl.cam.ac.uk/users/rja14/#SR`

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

1 Applications and Engineering

043101 'Two New Imaging Techniques Promise To Improve IC Defect Identification'
C Ajluni, *Electronic Design Vol 43 No 14 (10 July 1995) pp 37–38*

The article reports on the Light-Induced Voltage Alteration (LIVA) and Low-Energy Charge-Induced Voltage Alteration (LECIVA) techniques developed at Sandia National Laboratories. LIVA is a non-destructive technique that involves probing operating ICs from the back side with an infrared laser to which the silicon substrate is transparent. The photocurrents thus created allow probing of the device's operation and identification of logic states of individual transistors. LECIVA relies on a surface interaction phenomenon that produces a negative charge-polarization wave using a low-energy electron beam generated by a scanning electron microscope. This allows imaging the chip to identify open conductors and voltage levels without damage, although it does not operate through metalization layers (unlike the higher-energy, but more damaging, CIVA technique on which it is based).

043102 'Cryptographic Credit Control in Pre-payment Metering Systems'
RJ Anderson, SJ Bezuidenhout, *Oakland 95 pp 15–23*

The authors describe the introduction of cryptography to protect prepayment utility meters from token fraud. Instructions to the meter are encrypted under a meter unique key and conveyed using a token, which may be a magnetic token or a number which the customer enters in the meter. Various robustness problems were encountered when transferring this technology to Africa, and the security problems all involved blunders in design, implementation and operation, rather than high tech attacks, thus confirming the first author's analysis of fraud from ATMs (**031103**). Other lessons learned included the advisability of using multiple evaluators and field trials, and the difficulty of managing trust relations in multivendor systems.

043103 'Virtual payment — it's here'
M Baggott, *Scottish Banker (Aug 95) pp 34–35*

This article describes an online shopping service run by Barclays Bank whose security relies on that provided by Netscape.

043104 'Low cost fingerprint system for ATMs'
Banking Technology (July/Aug 95) p 48

This article describes a neural-network based fingerprint recognition device which cuts the cost of this technology to about £200 per unit.

043105 'Security in hospital information systems'
B Barber, D Garwood, P Skerman, *International Journal of Biomedical Computing v 39 no 1 (Apr 95) pp 133–138*

The authors discuss the European background to medical systems security, relate some of the perceived threats, and mention some of the committees involved in standards development work.

043106 'Improving system security via proactive password checking'
M Bishop, DV Klein, *Computers and Security v 14 no 3 (95) pp 233–249*

The authors describe pwcheck, a password checker supplied with their Unix passwd+ utility which trains users in password selection by identifying and rejecting weak password choices.

043107 'Techniques for Privacy and Authentication in Personal Communications Systems'
D Brown, *IEEE Personal Communications v 2 no 4 (Aug 95) pp 6–10*

In a journal version of **31403**, the author describes and contrasts the authentication and key agreement protocols used by GSM, the US Digital Cellular IS-41 standard, and the Beller-Yacobi scheme. There are now seven air interfaces under development by PCS standards bodies, most of which plan to use the GSM or IS-41 protocols. While GSM uses individual challenge-response, IS-41 mobiles must respond to a global challenge in their call setup request. This makes the over-air protocol simpler, at the cost of more problematic key management between base stations.

043108 'Credit card security boosted by nuclear weapons program'
C Bucholtz, *Computer Fraud and Security Bulletin (July 95) p 9*

Los Alamos is working on pattern detection software for Mastercard; this will spot anomalous credit card transactions using neural network and other techniques developed to spot evidence of clandestine nuclear weapons programmes.

043109 'Fraudsters had less success last year'
Cards International (3/8/95) p IV

Mastercard International reported fraud down to $486m in 1994 while sales were up at $389.9bn. Lost and stolen cards declined, as did mail fraud; counterfeiting was up 24.3% to $166m. 90% of cards now feature CVCs — crypto checksums on the mag strip — while VISA, which introduced these a year earlier, had fraud down to $645m on turnover of $631bn, with their counterfeit losses down 6% at $146m.

043110 'Europe becomes largest ATM market'
Card World Independent (July 95) p 3

According to a 1994 survey, Europe has 133,184 ATMs, overtaking Japan's 122,415, while the USA has just broken the 100,000 mark and the total worldwide is about 425,000, growing at 13% per annum. A third of Europe's new installations were in Germany, which has 24.382 machines; Spain is second with 23,292 and the UK is third with 19,377. The highest ATM density per population is in Finland, and the largest transaction volume is in the UK. However, the number of withdrawals per terminal per month has been declining since 1989.

043111 'UK ID card update'
Card World Independent (July 95) p 8

Despite the show of consultation, the UK government is pressing ahead with the introduction of identity cards. These will be introduced as drivers' licences and pension/welfare benefit cards; eighty percent of the population will thus be issued with them soon, whether they like it or not.

043112 'UK travel networks share smart ticketing system'
Card World Independent (June 95) p 6

Under an EC contract, buses in Harrow, West London, have been using contactless smartcards with photos as 'farecards'; these allow an hour's travel, including transfers, for a pound. The system is now being extended to all London, and will reduce fraud by exit monitoring and by preventing the use of stolen and outdated cards. It will also speed boarding.

043113 'Coming of age but industry remains to be converted'
R Carter, *Fraud Watch (summer 95) pp 6–8*

The author surveys biometric techniques, and automatic fingerprint recognition in particular. Skin damage suffered by pipesmokers and manual workers is one source of error; another is hand cream, which can clog grooves. Error rates can be reduced by looking at patterns of skin pores as well as at the more conventional minutiae, or by reading the print using ultrasound rather than light.

043114 'Keep it safe'
J Charlton, *Computer Weekly (28/9/95) p 48*

Three UK firms are now offering remote backup — a system which scans client

LANS every day for new programs or data, then automatically compresses and encrypts copies of these files and ships them offsite for backup.

043115 'Security Challenges in NII'
YM Chee, SH Goh, *Information Technology — Journal of the Singapore Computer Society v 6 no 1 (Sep 94) pp 43–50*

The authors describe the security architecture of Singapore's National Information Infrastructure. The basic building blocks are that each user will have a subject sponsor (an entity aware of all his activities), and use an authentication service to prove his identity to network resources. There will be facilities for association management (authorising entities to communicate on certain paths), a security state facility to track all currently active subject/object relationships, and facilities for security attribute management, interdomain attribute mapping, cryptography, authorisation, audit, and security recovery.

043116 'Developing and Deploying a Corporate-Wide Digital Signature Capability'
DE Coe, FJ Smith, *ACM SIGSAC v 3 no 3 (July 95) pp 5–8*

The authors describe a digital signature architecture being deployed at MITRE in Q3 95. This will use DSA to talk to government, and RSA to talk to industry; central private key generation, with private keys and passwords stored on conspicuously coloured diskettes; and an in-house certification authority, with certificates based on X.509 and valid for three years.

043117 'Security Challenges for the Banking Industry'
L Collins, *CPAC 95 pp 113–134*

The author describes the crypto policy and architecture of the Commonwealth Bank of Australia. This is based on smartcard access control devices, DES cards for hard disk encryption, and an access control architecture based on OS/2 and NT which is targetted at a C2 level of assurance. Value transactions are MACced, and sensitive fields are encrypted.

043118 'Perceived acceptability of biometric security systems'
F Deane, K Bardle, R Henderson, D Mahar, *Computers and Security v 14 no 3 (95) pp 225–231*

The authors present the results of a survey of banking and university staff attitudes to biometric identification. All systems were perceived as less acceptable than passwords, but the behaviourally based systems were significantly less acceptable than the physiological ones. There may be a link with employee concerns over performance monitoring systems.

043119 'Sicherheit und Elektronische Unterschriften — SmartDisk'
R Eisele, *Datenschutz und Datensicherung (7/95) pp 401–406 (in German)*

The author describes SmartDisk, a device which contains a smartcard crypto engine (with public key capability) but is packaged like a 3.5 inch diskette, and has electromagnetic circuitry which enable a PC to read and write it. This provides smartcard capability without the need for a smartcard reader.

043120 'Bankers' trust encourages key escrow'
E English, *Computer Fraud and Security Bulletin (July 95 pp 7–8*

This article reports a scheme devised by Bankers' trust under licence from MIT to provide corporate key escrow services.

043121 'From There to Here'
D Everett, *Smart Card News vol 4 (95); part 5: June pp 116–119; part 6: July pp 135–139; part 7: Aug pp 156–159*

This is a management level tutorial on smart cards covering fabrication, hardware and electrical interface standards.

043122 'Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunk-teilnehmern'
H Federrath, J Thees, *Datenschutz und Datensicherheit (June 1995) pp 338–348 (in German)*

The authors describe how direct sequence spread spectrum techniques can be used to make it harder for an eavesdropper to determine the physical location of a transmitter. Low-probability-of-intercept systems use cryptographic rather than maximal length spreading sequences; a direction finding apparatus would need to do a autocorrelation or crosscorrelation analysis of the sequence in order to select the signal. By comparison, frequency agile systems are relatively easy to intercept. There are a number of other engineering factors which need to be considered when designing anonymous networks, such as computer security measures to protect location information stored in the network, and dummy traffic to preventing active attacks through the network. Call setup is troublesome, particularly when initiated by the mobile station; the most elegant solution involves Rabin's beacons.

043123 'Rise in fraudulent accounts as counterfeit drops'
Fraud Watch (summer 95) pp 2–3

As CVC/CVV codes have made credit cards harder to forge, the villains are turning to fraudulent account opening. The typical modus operandi is to change a victim's address to a drop address and then apply for a credit card in his name. In consequence, there is no prospect — at least in the USA — of justifying chip cards from fraud savings alone.

043124 'US phone-related fraud flourishing'
Fraud Watch (summer 95) p 5

This article describes frauds carried out by crooked phone companies against customers, especially where long-distance charges are billed through local carriers. There are also sharp business practices, such as charging fraudulent calls to customers.

043125 'The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image'
GL Friedmann, *IEEE Transactions on Consumer Electronics v 39 no 4 (Nov 93) pp 905–910*

The author describes how to embed a signature capability in a digital camera for forensic applications. He suggests that a secure processor with signing keys be embedded in the camera at manufacture; the signature would secure not just the image, but also the time and data, light level, colour temperature, focusing distance and maybe even GPS location data. All this additional information would be held in a strip at the side of the picture.

043126 'Integrating Smart Cards into Authentication Systems'
G Gaskell, M Looi, *CPAC 95 pp 263–279*

The authors discuss alternatives for fortifying Kerberos with smartcards and public key techniques. Smartcard storage of passwords and/or session keys gives immediate gains, but most existing smartcards do not support modular exponentiation. Thus when public key is advantageous, the best compromise may be to store the secret key on a card and do decryption/signature functions in the card reader. The risks and benefits of these choices are discussed in the context of EDI.

043127 'Payment Switches for Open Networks'
DK Gifford, LC Stewart, AC Payne, GW Treese, *CompCon 95 pp 26–31*

The authors describe a payment system which aims to reduce the cost to banks of insuring customers and merchants from each other by making payments against digitally signed instructions to external accounts through a billing server. The payment protocols are outlined.

043128 'Quantum Cryptography Based on Orthogonal States'
L Goldenberg, L Vaidmar, *Physical Review Letters v 75 no 7 (14/8/95) pp 1239–1343*

Previous quantum cryptosystems had used nonorthogonal states to carry information, since these cannot be cloned and an eavesdropper must therefore introduce errors. The authors introduce a new scheme based on orthogonal states; the idea is to use superpositions of two localised wave packets, one of which is delayed for a fixed time in a storage ring, and to send the packets at times which are unpredictable to the eavesdropper.

043129 'An automatic seal imprint verification approach'
Q Hu, JY Yang, Q Zhang, K Liu, XJ Shen, *Pattern Recognition v 28 no 8 (Aug 95) pp 251–266*

Documents in China and some other Eastern countries are authenticated by seal imprints rather than by signatures, and the manual verification of these is both time-consuming and error prone, leading to serious bottlenecks in document processing. The authors discuss the problems of recognising seals automatically and of distinguishing genuine seals from typical forgeries. They describe a system developed for cheque verification by the biggest domestic bank in China; this takes about one second per seal on a 486 PC, and has been successfully fielded with a relatively low false reject rate (2%).

043130 'Optical Character Recognition for Self-Service Banking'
LD Jackel, D Sharman, CE Steward, BI Strom, D Zuckert, *AT&T Technical Journal v 74 no 4 (Jul/Aug 95) pp 16–24*

The authors describe the development of the AT&T 5665 automatic teller machine which contains OCR technology to read cheques being deposited. New techniques had to be developed to get acceptable performance in this environment; the recognition engine is based on a neural network.

043131 'Biometrics: Is It a Viable Proposition for Identity Authentication and Access Control?'
HJ Kim, *Computers and Security v 14 no 3 (95) pp 205–214*

The author looks at the various biometric technologies available on the market and discusses some of the problems, such as error rates and privacy intrusion, which have prevented them fulfilling their early promise.

043132 'Bolero — a practical application of trusted third party services'
J King, *Computer Fraud and Security Bulletin (July 95 pp 12–15*

Bolero is an EU funded project to develop electronic bills of lading. These confer ownership of cargoes, so they must not be duplicated; a central registry is used to ensure that the name of the unique holder can be determined at all times. Public key crypto is used to achieve nonrepudiation of instructions, and further trusted third party services provide a registration authority (which vets the credentials of organisations) and a certification authority (which signs the public keys of individuals authorised by registered organisations).

043133 'Neue Sicherheitskonzepte von Point-of-Sale (POS)-Systemen'
A Kiranen, *Datenschutz und Datensicherung (1/95) pp 35–44 (in German)*

The author provides an overview of ETFPOS concepts and systems architectures, together with a large bibliography. EFTPOS is just starting to take off in Germany.

043134 'Towards Robust and Hidden Image Copyright Labeling'
E Koch, J Zhao, *NSIP 95 pp 452–455*

The authors describe a system they developed to hide copyright messages in JPEG compressed digital images. These messages are robust in the fact of lossy compression and low pass filtering; they are encoded at a number of locations in the picture which are determined by a secret key.

043135 'Chipkarte und Sicherheit'

D Kruse, H Peuckert, *Datenschutz und Datensicherung (3/95) pp 142–149 (in German)*

The authors present an overview of chip cards and describe how they may be used for access control, digital signature, secure communications, electronic payments and medical records.

043136 'Integration of Intelligent Network Services into Future GSM Networks'

M Laitinen, J Rantala, *IEEE Communications Magazine v 33 no 6 (June 95) pp 76–86*

The authors describe the architecture of GSM, including signalling, routeing, and authentication; list a number of services and data modes which should be available in GSM phase 2; and discuss how the future Universal Personal Telecommunications (UPT) service may be layered on top of GSM networks. Eventually, a single smart card may give access to a range of services — GSM, DECT and other future mobile services — and regardless of the network used, the customer will have a single number and get a single phone bill.

043137 'Cryptology for Digital TV Broadcasting'

BM Macq, JJ Quisquater, *proceedings of the IEEE v 83 no 6 (June 95) pp 944–956*

The authors discuss the distinguishing features of crypto for digital TV. The information rate is much higher, the value is much lower, and the interaction with underlying protocols such as MPEG is more complicated, than in other applications. For example, the crypto must be resynchronised along with each I-frame of MPEG, or channel switching latency will rise; and the overall system design must cope with transcoding, such as from 10Mbit/sec to 3Mbit/sec at the head end. They propose some engineering principles, such as that all capabilities must be time limited; describe some of the routine management and control messages, and discuss design considerations for the key hierarchy and for the overall broadband network.

043138 'On the Penrose hypothesis on fingerprint patterns'

KV Mardia, Q Li, TJ Hainsworth, *IMA Journal of Mathematics Applied to Medicine and Biology v 9 no 4 (1992) pp 289–294*

Penrose hypothesised that fingerprint patterns are formed according to the curvature of the embryo's skin at the time of ridge formation. A differential equation derived for this by Smith is solved and extended to explain all the important patterns. It turns out that the ridges may follow the lines of stress rather than curvature.

043139 'The big shake-down'

R Martin, C Power, *Cards International (28/8/95) pp 8–19*

This article is a detailed survey of the plastic card market in the UK, covering bank, affinity and T&E cards. It lists the numbers in issue, transaction volumes and values, and fraud rates.

043140 'Video-Steganography: How to Secretly Embed a Signature in a Picture'

K Matsui, K Tanaka, *Journal of the Interactive Multimedia Association Intellectual Property Project, v 1 no 1 (Jan 1994) pp 187–205*

The authors discuss schemes to embed copyright messages in pictures compressed using a number of different signal processing schemes, including predictive coding, ordered dithering, facsimile and discrete cosine transform. For example, fax messages are signed by replacing the rightmost pixel of each line with the next bit of the signature.

043141 'Hackers exploit weakness in anti-abuse software'

M McCormack, *Computer Fraud and Security Bulletin (July 95) pp 1–2*

Most carriers' abuse detection software does not get invoked until a call is completed and billed. Hackers have discovered this and are now using stolen calling card numbers to make calls in excess of a hundred hours long.

043142 'The CASS Shell'
G Mohay, Q LeViet, H Morarji, *CPAC 95 pp 347-365*

The authors developed a Unix shell which checks that programs have not been corrupted before executing them. The main mechanism is that each user has a virtual root, and the rest of the file store is hidden. New programs and shell scripts can be checked for dangerous constructs before being added to the list of authorised executables.

043143 'Development and Performance of Unix Encryption Services'
H Morarji, L Munday, W Caelli, *CPAC 95 pp 329–346*

The authors discuss the problems encountered while porting device drivers for the Eracom PC-ASM DES encryption card from SCO Unix to SVR4.2. The differences between Microsoft and AT&T assemblers and the differences between the two kernels were the most troublesome aspects of this project.

043144 'Requirements for Network Payment: The NetCheque Perspective'
BC Neuman, G Medvinsky, *CompCon 95 pp 32–36*

The authors describe their system for network payments. It is a cheque system with certain anonymity properties; it was originally designed to maintain quotas for distributed system resources, and runs on top of Kerberos whose tickets it uses for authentication purposes.

043145 'Nipping fraud in the bud'
J Newton, *Cards International (11/7/95) p 8*

The author reports on a card fraud seminar in Turkey, where losses are still mostly in Istanbul and the tourist regions.

043146 'GP Practice computer security survey'
RA Pitchford, S Kay, *Journal of Informatics in Primary Care (Sep 95)*

The authors carried out a survey of computer security among 144 British general practitioners. Half of all practices had their systems connected to the outside world; administrative staff with access outnumbered clinicians by two to one; and four fifths of practices had a computer manager. Security awareness was generally high. For example, 84% thought a computer security policy important; 90% thought security awareness training for staff to be very important; and 74% thought it important or very important to tell patients when their data had been passed to third parties. Over 10% reported having had computer hardware stolen.

043147 'Do you take cybercash?'
C Power, *Cards International (14/6/95) p 7*

At present, US retail sales are about $1.5 trillion, of which $53bn is due to catalogue shopping, $2.5bn to home banking and $200m to online ordering. The three largest players in the last of these segments are Compuserve with 3m subscribers, AOL with 2.7m and Prodigy with 1.7m. A number of alliances are being formed to develop things.

043148 'Europay plugs into the Internet'
C Power, *Cards International (22/6/95) p 5*

Europay will run a payment pilot over the web in 1996 which will use IBM's iKP protocol together with an electronic purse from Europay.

043149 'Auditable Random Numbers'
S Roberts, *CPAC 95 pp 105–112*

The author describes some of the techniques used to generate key material at the ANZ bank group. These include having three people type random text, too quickly for them to remember it, distilling 1 bit per character, and adding together the three components this process yields. They have also used large sheets printed with thousands of odd parity bytes.

043150 'Road-Pricing-Systeme und Datenschutz'
A Roßnagel, U Pordesch, *Datenschutz und Datensicherung (2/95) pp 77–86 (in German)*

Electronic road pricing is currently under trial in Germany and elsewhere, and should be fielded by 1998. Some possible system architectures are described; the main data protection problem is to prevent the tracking of vehicle movements, but all systems keep toll data as this is needed to prosecute nonpayers. German law on police access for other purposes is discussed. There appears to be a serious risk that data protection in the eventually fielded systems will be farcical unless more work is done on the interplay between technical and legal aspects.

043151 'Implementing Separation of Duties with an AI Cosignature Controller'
S Russell, *CPAC 95 pp 143-148*

The author proposes that when implementing threshold signature and other shared control schemes, a blocking share should be retained by a server whose duty is to verify that the document has been signed by an authorised pattern of signers. This could provide a convenient place to locate a sanity check on document contents as well as an alarm and revocation facility.

043152 'The Intel 80x86 processor Architecture: Pitfalls for Secure Systems'
O Sibert, PA Porras, R Lindell, *Oakland 95 pp 211–222*

Traditionally, compusec evaluations have paid little attention to hardware. However most products evaluated B2 or above use Intel processors, and this motivated the authors to look for potentially exploitable hardware features. They found covert channels in the Task Switched flag, segment attributes, interrupt descriptor tables, debug registers, the time stamp counter, and performance counters. Caches can also provide covert channels, and in addition to all these design features there have been a number of implementation errors reported, including freak security flaws. There are also a number of subtle traps for TCB implementers. Thorough analysis is made more difficult by the fact that the processor implementation details are secret.

043153 'NetBill: An Internet Commerce System Optimized for Network Delivered Services'
M Sirbu, JD Tygar, *CompCon 95 pp 20–25*

The authors describe an electronic commerce system designed to have low transaction costs for small payments and to be highly scalable. It is aimed particularly at online delivered goods such as decryption keys for software.

043154 'NetBill: An Internet Commerce System Optimized for Network Delivered Services'
M Sirbu, JD Tygar, *IEEE Personal Communications v 2 no 4 (Aug 95) pp 34–39*

This is the journal version of the above.

043155 'Electronic Purses: A Comparative Review'
Smart Card News (Aug 95) pp 145–149

This article tabulates the features of electronic wallets in Belgium, Denmark, Finland and Latvia.

043156 'Review of Contactless Cards'
Smart Card News (June 95) pp 105–109

This article tabulates the features and characteristics of 13 contactless smartcards from nine manufacturers.

043157 ‘UK Road Toll Trials’
Smart Card News (Aug 95) pp 150–151

The UK Transport Research Laboratory will run trials of road toll systems proposed by eight different consortia on the M3 near Basingstoke for two years from 1996.

043158 ‘Trials of Wireless, Secure Electronic Mail’
DR Smith, SD Simon, LE Cautille, *IEEE Personal Communications v 2 no 4 (Aug 95) pp 28–33*

The authors describe a pilot project by the US Department of Defense to integrate email — using Microsoft Mail and Lotus cc:Mail — with CDPD and older packet radio networks, using commercially available DES software and then Fortezza cards to protect the traffic. Future developments will include the use of existing worldwide military HF and future commercial satellite networks.

043159 ‘Multimedia millions through virtual banking’
J Smith, *Scottish Banker (Aug 95) pp 32–33*

This article describes a pilot project by Nationwide in which 20 machines have been installed in eight branches to dispense marketing information and provide video links to sales staff.

043160 ‘Holding Intruders Accountable on the Internet’
S Stanford-Chen, LT Heberlein, *Oakland 95 pp 39–49*

The authors’ problem is to detect intruders who are chaining a session through a series of computers on a network, and their solution is to use a principal components analysis of character frequency to determine whether two connections are part of the same chain. By using the second through seventh components of the variance, they obtain a session thumbprint which requires only 24 bytes per minute.

043161 ‘Airborne signals intelligence’
M Streetly, *International Defense Review v 28 (July 95) pp 39–42*

This article discusses the transition of airborne sigint from the cold war model to the new world of international policing operations. The Gulf war saw the first serious attempts to incorporate sigint tightly into operations. The systems used by a number of countries, including the USA, South Africa, Israel and the UK, are described.

043162 ‘CommerceNet: Spontaneous Electronic Commerce on the Internet’
JN Tenenbaum, C Medich, AM Schiffman, WT Wong, *CompCon 95 pp 38–43*

The authors describe CommerceNet, a consortium set up to facilitate business transactions over the Internet. These include bids, directory searches, production scheduling, and establishing design partnerships; the underlying mechanism is expected to be shttp.

043163 ‘Broadband Networks and Services: Architecture and Control’
MP Vecchi, *IEEE Communications Magazine v 33 no 8 (Aug 95) pp 24–32*

This article summarises the IEEE Broadband 95 Workshop, and covers a number of topics including the CORBA framework and authentication.

043164 ‘Strong Theoretical Steganography’
P Wayner, *Cryptologia v XIX no 3 (July 95) pp 285–299*

The author proposes a system of steganography based on context free grammars. Learning a van Wijngaarden grammar is equivalent to a Turing machine. In a practical system, input ciphertext bits can be used to select productions from the grammar, and can be recovered through parsing so long as the grammar is unambiguous. An example is given based on English text generated using these ideas.

043165 'Privacy and Authentication Needs of PCS'
JE Wilkes, *IEEE Personal Communications v 2 no 4 (Aug 95) pp 11–15*

The author discusses the protection requirements of PCS telephones, and covers the privacy of content, location, call pattern and signalling. Devices must also have the authenticity property of resisting cloning attempts, both at installation and repair. Some jam resistance is also advisable, and law enforcement access is also discussed.

043166 'Retailer aspirations in plastic cards and payment systems'
S Worthing, *Journal of retailing and Consumer Services v 1 no 1 (July 94) pp 30–39*

The author discusses the power relationship between retailers and banks, and the effect on it of technology. Retailers wish to enter into the payment chain in order to collect marketing information, run loyalty programmes and cut the margin paid to the banks, whereas banks seek to prevent this. Five case histories from four different countries are presented; these show that dominance can shift between different members of the chain, and is usually based on a combination of two or more factors such as money, coercive ability, expertise and helpfulness. As a last resort, merchants (or groups of merchants) may become card issuers in order to break the banks' dominance.

043167 'Embedding Robust Labels Into Images For Copyright Protection'
J Zhao, E Koch, *IPR 95 pp 242–*

The authors describe two copyright marking schemes — one for embedding labels in JPEG compressed images, and one for black and white images. The former alters the quantisation table in the discrete cosine transform, and the latter encodes a bit according to whether a block of pixels is more black than white. Varying the table or block size allows the tradeoff between robustness and visibility to be selected.

2 Operating System and Database Security

043201 'A higher level of security through active policies'
MD Abrams, JD Moffett, *Computers and Security v 14 no 2 (95) pp 147–157*

The authors argue that the conventional reference monitor is too passive, and suggest adding a situation monitor which would tighten access rules at times of perceived threat; the input for this might come from an intrusion detection system. They claim that this would force designers to analyse and codify those security management tasks which are now left to the administrator's discretion.

043202 'Assessing Computer Security Vulnerability'
J Alves-Foss, S Barbosa, *Operating Systems Review v 29 no 3 (July 95) pp 3–13*

The authors propose a standard way to assess the vulnerability of discretionary access control systems where the threat model is that outsiders may become users, and users superusers, by exploiting the standard kinds of implementation and administrative slackness.

043203 'Practical Domain and Type Enforcement for Unix'
L Badger, DF Sterne, DL Sherman, KM Walker, SA Haghighat, *Oakland 95 pp 66–77*

The authors wished to escape the overheads associated with the low level access checks inherent in traditional type enforcement mechanisms. They therefore implemented a prototype domain and type enforcement system; domains are somewhat like roles and are expressed in a high level language. They report real security gains while retaining a lot of compatibility with existing systems.

043204 'Connection Policies and Controlled Interference'
WR Bevier, RM Cohen, WD Young, *CSFW 95 pp 167–176*

The authors describe a generalization of their work on intransitive non-interference. Typical intransitive noninterference requirements are at the granularity level: whether agents may or may not interfere. Controlled noninterference permits a finer granularity by using connection policies to define what channels connect agents, and effectively capture how agents may or may not interfere with each other. They conclude by examining related work on intransitive noninterference, separability and type enforcement (assured pipelines).

043205 'Extended Abstract: An Architecture for Covert Channel Control in RealTime Networks and MultiProcessors'
R Browne, *Oakland 95 pp 155–168*

The author introduces an architecture for dealing with covert channels in multilevel realtime networks and multiprocessor systems. He proposes a 'systolic, elastically separable' system; systolic means phase-delayed I/O and non-preemptive scheduling, while elastically separable means that each multilevel task can be rewritten as a fixed, finite sequence os single level tasks which read down but do not write up, and such that only tasks at the highest level in the system refer to a realtime clock. He shows that such systems confine covert communication in useful ways.

043206 'The Semantics and Expressive Power of the MLR Data Model'
F Chen, RS Sandhu, *Oakland 95 pp 128–142*

The authors provide a new semantics for multilevel relational databases which is data based rather than based on the beliefs of subjects. Their basic idea is to differentiate between data which is owned by the subject (and thus reliable) and data which is borrowed from lower level subjects (and thus liable to change). This is efficient in the common case where 95% of secret information merely replicates unclassified items. Its five principles are entity and foreign key integrity (both borrowed from SeaView), polyinstantiation and referential integrity (upgraded from the second author's previous work), and a new principle of 'data-borrow integrity', which means that low-level data changes are propagated upwards efficiently.

043207 'Supporting Security Requirements in Multilevel Real-Time Databases'
R David, SH Son, R Mukkamala, *Oakland 95 pp 199–210*

In a MLS DBMS it is well known that the ability of High to abort/slow a Low transaction can covertly signal information. The authors discuss how spurious aborts can lessen the covert channel capacity and the impact of these additional aborts upon system performance. In this paper, the term "capacity" is used in place of "mutual information" and the probabilities for calculating the entropies are incorrect; the authors are working on a revision.

043208 'Integrating Security in CORBA Based Object Architectures'
RH Deng, SK Bhonsle, WG Wong, AA Lazar, *Oakland 95 pp 50–61*

The authors propose a distributed security architecture based on trusted object request brokers which could be incorporated into CORBA based systems.

043209 'The Security Checker: A Semantics-based Tool for the Verification of Security Properties'
R Focardi, R Gorrieri, V Panini, *CSFW 95 pp 60–69*

The authors describe work on adapting the CCS Concurrency Workbench to model-check information flow properties of CCS style specifications. The checking algorithms have poor (some exponential) worst case complexity results. However, in practice the authors have found the time and space requirements for the algorithms to be reasonable, especially if algebraic properties (for example, parallel composition) of the security property are used to reduce the number of states to be checked.

043210 'Specifying Security for CSCW Systems'
SN Foley, J Jacob, *CSFW 95 pp 136–145*

The authors describe a method for specifying functionality and security (confidentiality) requirements for CSCW applications. Testing the method against a simple case study, they were surprised that security turned out to be very simple to specify. They suggest that this came about as a result of the way the application is modularized, and because so much is captured by the functionality requirements.

043211 'A Multilevel File System for High Assurance'
CE Irvine, *Oakland 95 pp 78–87*

When designing multilevel applications, the designer must not only observe policy constraints but also use and trust the TCB, rather than building new security mechanisms outside it. However, many existing MLS products have extremely primitive application programming interfaces, and the author describes a system which was designed to tackle this problem. For example, it makes it easy for application programs to create new access classes when required.

043212 'Implementation of a Discretionary Access Control Model for Script-based Systems'
T Jaeger, A Prakash, *CSFW 95 pp 70–84*

The authors propose an access control model tailored specifically for script based systems. The model provides roles for processes running command scripts: accesses are determined by the rights of the process and script author. The model has been implemented using Safe-Tcl under Kerberos and Taos.

043213 'The INCINERATE Data Model'
HV Jagadish, *ACM Transactions on Database Systems v 20 no 1 (Mar 95) pp 71–110*

The author presents an extended relational algebra for database systems in which universally quantified classes can be expressed as attribute values. This can be built on top of a standard relational database, it can support lattice models of inheritance, and significantly reduce the database size in certain applications.

043214 'Building Higher Resolution Synthetic Clocks for Signaling in Covert Timing Channels'
JVA Janeri, DB Darby, DD Schnakenberg, *CSFW 95 pp 85–95*

The authors describe a network LAN covert channel, and its countermeasures, based on process scheduling. Controlling the channel by adjusting clock granularity can conflict with the timing requirements of network software. This was exemplified by the discovery of an Heisenberg-like principle: the covert channel worked when debugging code was present in the software, but decayed when it was removed!

043215 'Concurrency Control for Federated Multilevel Secure Database Systems'
IE Kang, TF Keefe, *CSFW 95 pp 118–135*

The authors are building federated multilevel DBMS on top of autonomous, pre-existing multilevel DBMS systems. Their approach uses a secure validation protocol which ensures serializability across the federation, maintains local autonomy of individual DBMS and ensures multilevel security. While their protocol currently requires the security lattices of local DBMS's to be total, the resulting lattice for the secure federation is not necessarily total. They also have a novel method for untrusted timestamp generation that can be used in their protocol.

043216 'A Network Version of the Pump'
MH Kang, IS Moskowitz, DC Lee, *Oakland 95 pp 144–154*

The authors show how to extend the NRL data pump from a single system into a distributed one. The basic pump keeps a buffer and emits ACKs to Low at probabilistic times based on a moving average of the ACK times from high; this is extended to multiple buffers at both Low and High levels. One must pay attention to congestion control issues; if inputs could send messages faster than outputs could handle them, then covert channels would open up.

043217 'Algebraic Properties of System Composition in the LORAL, Ulysses and McLean Trace Models'
AP Manecki, *CSFW 95 pp 16–21*

The author gives a catalogue of algebraic properties (such as associativity and commutativity) for the information flow properties of Dinolt, McCullagh and McLean. His conclusion is one of caution: one should be mindful of how compositions are made, even if the property is composable in principle, as algebraic properties may fail in the presence of feedback.

043218 'Composing and Decomposing Systems under Security Properties'
AW Roscoe, L Wulf, *CSFW 95 pp 9–15*

The authors argue that a more expressive model than traces should be used when capturing information flow properties in CSP. They studied separability, and its relationship to composition, in terms of the failures-divergences model, and concluded that separability is not a sound property for systems that have (internal) nondeterminism.

043219 'Management von Sicherheitsdiensten in verteilten Systemen'
M Steiner, G Kurjoth, R Hauser, *Datenschutz und Datensicherung (3/95) pp 150–155*

The authors describe SAMSON, an IBM architecture for security management in distributed systems which follows the OSI model and was developed within the EU's RACE project. It is based on a managed object hierarchy, which includes a registry of managed objects and a security policy, and it integrates audit with the authentication mechanisms.

043220 'The Epistemic Representation of Information Flow Security in Probabilistic Systems'
PF Syverson, JW Gray, *CSFW 95 pp 152–166*

The author outline a logic for security in which information flows due to time and probability can be accounted for. Their logic, built on the standard Halpern-Tuttle model of knowledge and probability in systems, represents a bringing together of previous work in the areas of noninterference and epistemic logic.

043221 'Java and Internet programming'

A van Hoff, *Dr Dobbs' Journal (Aug 95) pp 56–61*

The author describes Java, a programming language developed by Sun Microsystems which facilitates software distribution over the Internet. Its security features enable code to be downloaded and executed in relative safety.

043222 'Capacity Estimation and Auditability of Network Covert Channels'

BR Venkatraman, RE Newman-Wolfe, *Oakland 95 pp 186–198*

The authors continue their research into how the type, amount, and timeliness of data traffic on a network can be used to send covert information. They discuss their work in light of Browne's ideas of mode security. An audit threshold is analyzed with respect to the maximal damage due to the above types of covert channels. A study of the University of Florida network shoed that attempts to monitor traffic patterns in detail generated unmanageable amounts of data. Further details can be found in the first author's dissertation.

043223 'Version Pool Management in a Multilevel Secure Multiversion Transaction Manager'

AC Warner, TF Keefe, *Oakland 95 pp 169–182*

This paper develops an analytic model examing how many previous versions of a data item should be kept on hand. The model balances the needs of secure transactions with that of recoverability. Experiments are run on this model and a statistical analysis of the outcomes is discussed. The paper is a report on the first part of a prototype MLS DBMS based upon a scheduling protocol of Keefe and Tsai.

043224 'The Composability of Non-Interference'

A Zakinthos, ES Lee, *CSFW 95 pp 2–8*

The authors prove McCullagh's conjecture that noninterference is composable in the absence of feedback, and propose a novel, composable, non-interference property that permits a degree of feedback. They argue that non-interference is more appealing than restrictiveness, because it has a more intuitive feel and a larger class of systems satisfy the property.

3 Security Management and Policy

043301 'A Dutch Enciphered Code'
D Alvaréz, *Cryptologia v XIX no 3 (July 95) pp 261–264*

The author describes an enciphered code system used by Dutch diplomats from the 1880s until the 1930s. It used a French commercial code, which was repaginated for secret messages.

043302 'The Real Security threat: The Enemy Within'
M Alexander, *Datamation v 41 no 13 (15/7/95) pp 30–38*

Most computer security incidents involve insiders, and a number of tales of woe are recounted in this article.

043303 'Saving Dollars Makes Sense of Crypto Export Controls'
M Ames, *CPAC 95 pp 61–64*

The author discusses the issues of algorithm strength and escrow in terms of the economics of wiretapping. He predicts that the ITAR restrictions will be removed once enough foreign firms protect their communications to make export restrictions uneconomic; at that point, US firms will be encouraged to compete aggressively for offshore crypto business.

043304 'Crypto in Europe — Markets, Law and Policy'
RJ Anderson, *CPAC 95 pp 41–54*

The author reviews the law and policy on encryption in the UK, France, Germany and a number of other countries. He also lists the main markets for cryptographic equipment in Europe by sector. He concludes that the policy concerns are misplaced; most commercial crypto is about authenticity rather than secrecy, and the main problem is the reliability of cryptographic systems, particularly in evidence. There is little evidence that the availability of crypto will make much difference to the detection and prosecution of crime; however, when the reliability of bank systems can be challenged in court, then many prosecutions could fail.

043305 'Security issues in the EDI environment'
S Banerjee, DY Golhar, *Information Management and Computer Security v 3 no 2 (95) pp 27–33*

The authors discuss the vulnerabilities of EDI, and some shortcomings of the existing standardisation process.

043306 'Developing a Corporate Internet Policy'
K Beseke, *Network Security (July 95) pp 10–13*

About a fifth of corporations have a policy of not connecting to the Internet (though they often are without realising it). Another fifth are connected consciously, with a security policy in place. The remainder are connected in uncontrolled ways. A checklist of questions for such companies is presented.

043307 'Look on the dark side — it might just happen'
N Blackman, *Security Gazette (Aug 95) pp 25–26*

The author describes an integrated emergency planning exercise held at Coopers, at which representatives of all the emergency services met with corporate planners to work through the consequences of a hypothetical disaster — a light aircraft crash into their premises in London. Such exercises are being recommended to other companies.

043308 'Auswahlstrategien für Sicherheitsmechanismen zur Erfüllung von Sicherheitsanforderungen'
U Blöcher, A Pfau, *Datenschutz und Datensicherung (5/95) pp 284–292 (in German)*

The authors provide a guide to the choice of crypto mechanisms, and discuss the pros and cons of a number of algorithms, modes of operation and protocols.

043309 'Simplifying the state and federal computer crime law maze in the USA'
J Bloombecker, *Information Management and Computer Security v 3 no 1 (95) pp 18–20*

The author presents, in three large tables, the definitions, prohibitions and procedural provisions of the various US state and federal computer crime laws.

043310 'Classification of objects for improved access control'
HAS Booysen, JHP Eloff, *Computers and Security v 14 no 3 (95) pp 251–265*

The authors discuss a structured technique for making classification decisions about objects, which takes account of object dependencies.

043311 'Email fraud at universities'
C Bournellis, *Computer Fraud and Security Bulletin (Aug 95) pp 5–6*

The universities of Stanford and Michigan are working on an extension of PGP for automatically signing student email, in order to cut down incidents of fraud and harrassment.

043312 '20 Noted and Notorious Hacker Feats'
Byte (Sep 95) pp 151–162

This article recounts twenty of the best known hacking feats of all time.

043313 'Commercial Key Escrow: An Australian Perspective'
WJ Caelli, *CPAC 95 pp 3–30*

The author discusses some of the problems of key escrow, with particular emphasis on professional ethics as seen by the various bodies of computer professionals. A possible solution for Australia might be a combination of key certification by the post office and commercial data recovery centres which would give law enforcement access with a suitable warrant. Recovery centres might also be run by the post office.

043314 'Safeguarding databases: basic assumptions revisited'
R Cardinali, *Information Management and Computer Security v 3 no 1 (95) pp 30–37*

This article provides an introduction to the basics of computer security.

043315 'Legal aspects of software protection devices'
R Carolina, *Computer Law and Security Report v 11 no 4 (Jul-Aug 95) pp 188–193*

In a recent UK case (**023308**), a software developer was convicted of computer misuse when he inserted a timelock in his software; at least three US cases have also brought down judicial condemnation on developers for this practice. In all these cases, a commercial relationship had soured, and the developer used the lock to put the other party under duress. In general, the use of such devices appears to risk civil and criminal penalties unless the other party has consented in advance to their installation — and this consent is not held to be an unfair term in the contract.

043316 'Keep the Barbarians at the gateway'
P Cassidy, *Datamation v 41 no 11 (15/6/95) p 51*

The author provides an overview of Internet security issues.

043317 'On the Problem of Personal Data Protection in the Russian Federation'
D Chereshkin, A Kurilo, *Datenschutz und Datensicherung (8/95) pp 480–482*

Data protection is currently subordinate to national security and crime fighting in Russia; the ombudsman draws all his power from the President. The authors call for this to be changed, and legal safeguards independent of the executive, so that Russia can compete in the information market.

043318 'Why 32-bit Desktops Need Virus Protection'
F Cohen, *Datamation v 41 no 13 (15/7/95) pp 41–43*

Although 32 bit viruses appeared in 1992, they still do not propagate owing to the sparsity of hosts. However, the old 16-bit viruses will usually still work against the newer platforms, and 16-bit antivirus software does not work as well; so vigilance must not be relaxed.

043319 'Information Privacy'
G Collier, *Information Management and Computer Security v 3 no 1 (95) pp 41–45*

The author discusses the 1980 OECD guidelines on privacy, and the national legislation in Europe and elsewhere which has enacted these into national laws. The Australian Privacy Charter is discussed as an example.

043320 'Betrug durch Benutzung eines rechtswidrig erlangten Computerprogrammes'
Datenschutz und Datensicherung (8/95) pp 492–494 (in German)

A man was convicted of computer abuse in Germany and fined DM 2100 after using a computer program to get DM 105 from a gaming machine in a pub. His conviction was overturned on appeal, but reinstated by the Supreme Court on the grounds that the program he used exploited trade secrets of the machine's maker, namely a key which the maker had tried to protect; and that the right to be protected was that of the machine's operator to his income.

043321 'Organisational Security — Clean Up or Cover Up?'
J David, *Computers and Security v 14 no 2 (95) pp 99–101*

The author recounts a consultancy assignment for an unnamed international body where he was asked to look at external threats only; he found serious and easily fixable internal control problems, but was told that in order to get paid he would have to cut these from his report to avoid embarrassing staff.

043322 'Fraud — the corporate threat'
C Dickson, *Security Gazette (May 95) pp 29–30*

Half of all frauds are committed by a single insider working alone. Contributory factors include technology (such as PCs and copiers) which make it easy to produce plausible looking documents; competitive pressure on auditors which erodes their vigilance; the capture of regulators by the industries that they are meant to control; and the amateurism, dishonesty and greed of many top managers, which erodes the staff's sense of duty.

043323 'GATT, TRIPS and high tech'
S Doyle, *Computer Law and Security Report v 11 no 4 (Jul-Aug 95) pp 182–187*

The author explains the implications of the recent General Agreement on Tariffs and Trade for intellectual property, and in particular for software protection.

043324 'Why the cuckoo's egg might never have been written'
B Dwan, *Computer Fraud and Security Bulletin (July 95 pp 15–18*

The author assisted Stoll in the pursuit of Hess, as described in 'The Cuckoo's Egg', and gives his own version of events. Unlike Stoll, he was not impressed by Hess's skills, and argues that a competent hacker would not have got caught; as a result, the threat model commonly used is wrong as it underestimates the capability of serious system crackers.

043325 'Testing the disaster recovery plan'
B Edwards, J Cooper, *Information Management and Computer Security v 3 no 1 (95) pp 21–27*

The authors argue for a phased approach to DRP testing and offer some checklists.

043326 'Business continuity observations'
W Farquhar, *Computer Fraud and Security Bulletin (Aug 95) pp 9–15*

The author presents a structured approach to disaster recover planning.

043327 'A lawless frontier'
Financial Technology International Bulletin v XII no 2 (Aug 95) p 10

This article mentions some legal problems with electronic commerce in the UK. It suggests the introduction of a legal obligation on people to read their email regularly, and mechanisms to establish the jurisdiction in which an electronic contract was made.

043328 'Information Security Baselines'
KJ Fitzgerald, *Information Management and Computer Security v 3 no 2 (95) pp 8–12*

Desk top computing has very little installed or practised security. The author suggests some key controls to get the average firm started.

043329 'What if you had a flood in your computer room?'
K Fitzgerald, *Information Management and Computer Security v 3 no 1 (95) pp 38–40*

Flooding accounts for over 10% of computer disasters, yet is often overlooked or underestimated by planners. The experience of Dunlop Slazenger in a 1984 Sydney flood is recounted to emphasise the problems of recovery.

043330 'Battening down hatches'
P Green, *Banking Technology (July/August 1995) pp 36–40*

The author investigates the lessons learned by the London banks from the IRA bombings of the early 1990's, and describes the continuity planning work at Paribas.

043331 'The Barrett Review — Part II'
G Greenleaf, *Computer Law and Security Report v 11 no 4 (Jul-Aug 95) pp 204–205*

The author continues the discussion of the recent Australian government report on wiretapping from **042324**. This report's most controversial recommendation is that police and other agencies would have to notify innocent persons whose traffic had been intercepted within 90 days of the end of the investigation. The police fought this but their opposition was overruled in view of the fact that notification causes no real problems in the USA and Canada, where it is mandatory. It also raises the question of who pays for phone taps: agencies wanted the carriers to pay and recover the costs from their subscribers, but the report recommends that the carriers should recover them from the agencies.

043332 'Simple Social Engineering'
W Hancock, *Network Security (June 95) pp 13–14*

The author describes some experiments and experiences with social engineering — mainly using pretext enquiries on the telephone to obtain passwords. Authoritative pressure and the claim that a job needs to be done are often effective.

043333 'Zuit zum Umdenken'
W Hassemer, *Datenschutz und Datensicherung (8/95) pp 448–449 (in German)*

The author reviews 25 years of data protection in Germany. In the old days, the principal threat came from private interests, so it was natural for the state to provide protection; but the main threat now is from the growing international hegemony of government bodies, which suggests a shift from data protection to the privacy and autonomy of the individual. However, it is no longer feasible to limit policy to a single nation.

043334 'Business continuity planning'
K Hearnden, *Computer Audit Update part 3: July 95 pp 3–9; part 4: Aug 95 pp 3–13*

The author reports a survey of UK firms' attitudes to DRP including the proportion with a proper business impact analysis, and with a tested or at least viable plan; the regularity of testing; and the seniority of the manager responsible.

043335 'Risk Management & Corporate Security: A Viable Leadership and Business Solution Designed to Enhance Corporations in the Emerging Marketplace'
S Hill, M Smith, *Computers and Security v 14 no 3 (95) pp 199–204*

Emerging markets in India, China, the former USSR and elsewhere have a pervasive lawlessness that makes them into havens for risk. This must be factored into corporate computer, personnel and property risk management.

043336 'Data protection — developments and abuses'
S Hinde, *Computer Audit Update (Aug 95) pp 1–3*

This article reviews threats to UK data protection including reports by the Audit Commission and the last two data protection registrars. The explosion in the PC population was not foreseen, and may force a relaxation in registration requirements; while the development of a black market in illegal information led to the introduction, in section 161 of the 1994 Criminal Justice Act, of a new offence of procuring, selling or offering for sale information whose disclosure is not covered by a register entry.

043337 'Datensicherheit in UNIX-Rechnersysteme: Möglichkeit und Wirklichkeit'
M Hube, *Datenschutz und Datensicherung (2/95) pp 91–95 (in German)*

Unix systems can be secure if administered carefully, but they usually are not. A checklist for administrators is given.

043338 'Looking through the risk management window'
R Jacobsen, *Information Security Monitor (Aug 95) pp 5–8*

One is concerned with precisely two types of risk — low occurrence and high consequence, and high occurrence but low consequence. The reason for this is that low/low we don't care about, and high/high we wouldn't survive. The low/high type tend to recur after a generation, since people tend to dismiss risks which they have not personally experienced.

043339 'Suppliers beware: implementation of the unfair contract terms directive in Europe'
R Kemp, C Coulter, *Computer Law and Security Report v 11 no 4 (Jul-Aug 95) pp 194–198*

The authors describe a recent European directive which outlaws any contract term which 'contrary to the requirement of good faith ... causes a significant imbalance in the parties' rights and obligations ... to the detriment of the customer.' Its ramifications extent from electronic banking transactions through software licenses.

043340 'Riverbank laboratory correspondence, 1919 (SRH-050)'
L Kruh, *Cryptologia v XIX no 3 (July 95) pp 236–246*

The author presents and discusses some correspondence from 1919 which concerns a running key field cipher proposed by Mauborgne and solved by Friedman.

043341 'Smart Cards and Data Protection'
J Kuopus, *Datenschutz und Datensicherung (3/95) pp 164–167 (in German)*

The author discusses some European identification initiatives and calls for harmonisation of identification and data protection mechanisms.

043342 'Legal control of computer crime in Hong Kong'
MKO Lee, *Information Management and Computer Security v 3 no 2 (95) pp 13–19*

Hong Kong's approach to computer crime was not to create specific computer offences, but to extend the scope of burglary and criminal damage. This was done as recently as 1993; nonetheless Hong Kong was the first country in the Far East to tackle the problem. The law's provisions are described, and their effect compared with that of UK and US laws.

043343 'Internal auditors — the new Luddites'
K Lindup, *Computer Audit Update (Aug 95) pp 13–19*

The author discusses the ways in which internal auditors always seem to stand in the way of technological change, most recently in portable computing, electronic trading and the Internet. He warns that this is in general an unproductive strategy, and that auditors must adapt more quickly.

043344 'Data integrity and the Internet: implications for management'
RG Mathieu, RC Woodward, *Information Management and Computer Security v 3 no 2 (95) pp 3–7*

Citation of Internet sources in academic and industrial reports can harm the integrity and auditability of research work; even where sources persist, there may be contradictory versions available. Some guidelines are suggested.

043345 'Hacking: To Criminalize or Not? — Suggestions for The Legislature'
M Möhrenschlager, *Computers and Security v 14 no 2 (95) pp 103–112*

The author discusses whether hacking should be an offence in itself, or merely prosecuted as part of the wider offence of which it is a part, such as fraud, blackmail or espionage. He surveys the situation: Germany has laws about the unauthorised obtaining of information in general; the UK and many US states have specific offences, as do Norway and the Netherlands; while Austria, France and Canada have offences related to specific damage or fraud.

043346 'EDI and LAN — friends or enemies?'
S Ongetta, *Computer Fraud and Security Bulletin (Aug 95) pp 15–19*

The author describes some EDI systems and their general security requirements. The standard solutions to these can be fragile when run on local area networks.

043347 'Encryption and the global information infrastructure: an Australian perspective'
S Orlowski, *CPAC 95 pp 31–39*

The author sets out the Australian government position on crypto policy. The basic proposal is that private users should be restricted to low grade systems, while banks would have escrowed keys. In each case, a central decrypting unit would provide a data recovery function for local and federal police forces. There is some scepticism about the viability of escrow, as there is no market for better voice encryption than that provided by GSM; and work on ensuring the acceptance of digital signatures has largely been delegated to standards bodies.

043348 'Business interruption insurance: a vital ingredient in your disaster recovery plan'
TJ Paradine, *Information Management and Computer Security v 3 no 1 (95) pp 9–17*

The author discusses what can and cannot reasonably be insured, and the different ways in which loss of profits from a computer disaster can be assessed.

043349 'The mother of all safeguards'
DB Parker, *Computer Fraud and Security Bulletin (July 95 pp 9–12*

The author argues that the most important single security management measure is the mandatory incorporation of security accountability in managers' written performance reviews.

043350 'Euro-Clipper chip scheme proposed'

D Peachey, *Communications Week International no 151 (18/9/95) pp 1 & 81*

The author reports a Council of Europe recommendation to facilitate law enforcement access to communications and data within Europe. He claims that a EuroClipper scheme is getting under way.

043351 'The Fortress Mentality Part III: Tokens, One-Time Password Generators and the Roman Army'

P Peterson, *Network Security (June 95) pp 17–19*

The author continues his article on Internet security (from **034360-1**) with a brief history of passwords. The significant modern development has been the password sniffing attack; it is no longer enough for passwords to be hard to guess, they must also be hard to observe, leading to the rise of the handheld password generator. However, he warns that these devices will simply move the weakest point elsewhere, quite possibly to the user; he draws the analogy that improved car security led to the rise of carjacking.

043352 'Jail sentence for Email security breach'

F Rees, *Computer Fraud and Security Bulletin (Aug 95) pp 1–2*

An employee of Australia's attorney-general's department has been sentenced to nine months in jail for hacking the email system and attempting to pass documents to a third party.

043353 'Bedrohings- und Risikoanalysen bei der Entwicklung sicherer IT-systeme'

U Rosenbaum, J Sauerbrey, *Datenschutz und Datensicherung (1/95) pp 28–34 (in German)*

The authors discuss how to go from a risk analysis to a security specification. It is very important to iterate this as the system specification is refined.

043354 'Institutionell-organisatorische Gestaltung informationstechnischer Sicherungsinfrostrukturen'

A Roßnagel, *Datenschutz und Datensicherung (5/95) pp 259–269 (in German)*

The author criticises system designers and others who brush aside the legal and organisational problems of authentication with phrases such as 'trusted third party'. This has discouraged debate on the real issues, which include consumer protection, equal access to business facilities, liability for damages when things go wrong, the balance of public and private provision, the position of notaries and ID card officials, and of course parliamentary oversight of the whole business.

043355 'Take the Risk out of Wireless Communications'

P Ruber, *Datamation v 41 no 13 (15/7/95) pp 35–40*

The author discusses the risks of wireless devices such as pagers, cellular telephones and radio LANs. Battles raging over both technical standards and crypto policy are preventing effective open tools coming to market, although there are proprietary solutions from firms such as Apple and Sony.

043356 'Datenschutz in Netzen'

U Schlager, *Datenschutz und Datensicherung (5/95) pp 270–275 (in German)*

The author presents the Hamburg data protection office's guidelines on data security in networks.

043357 'Cryptanalysis for Peacetime: Codebreaking and the Birth and Structure of the United Nations'

S Schlesinger, *Cryptologia v XIX no 3 (July 95) pp 217–235*

Recently declassified documents show that the Americans solved the diplomatic cables of Argentina, Chile, France and other countries in the run up to the first UN conference in 1945. This helped them to get more or less the UN charter which they wanted.

043358 'Computerviren: Wer haftet wann?'
J Schneider, A Günther, *Datenschutzberater v 19 no 9 (15/9/95) pp 1–5 (in German)*
The authors discuss the liability for virus damage under German law. Employees can be held personally liable for negligence.

043359 'Factoring in Public-Key's Future'
B Schneier, *Byte (Oct 95) p 78*
The author discusses what lengths of RSA key will be needed under certain assumptions of opponent capability, cover time and progress with algorithms.

043360 'Promoting security awareness and commitment'
P Spurling, *Information Management and Computer Security v 3 no 2 (95) pp 20–26*
The author describes computer security management at Alcoa of Australia, a large alumina producer.

043361 'EC plans encryption rules in bid to police information superhighway'
J Thorel, *Nature v 377 no 6547 (28/9/95) p 275*
The author reports a European Union plan to provide governments with powers to decrypt confidential information. The guidelines are to be published in Autumn 95 and may include some form of key escrow. Opposition from civil liberties groups and others is reported, as is a parallel proposal from the Council of Europe.

043362 ' "Self Regulation" on the Internet'
A Taebi, *Computer Law and Security Report v 11 no 4 (Jul-Aug 95) pp 202–203*
The author contrasts the managerial and technical controls imposed, or proposed, for parts of the Internet; networks such as Microsoft's use moderators, while technical controls such as Clipper are advanced by external interests.

043363 'The book cipher system of the Wehrmacht'
M van der Meulen, *Cryptologia v XIX no 3 (July 95) pp 246–260*
The author describes a Wehrmacht system from 1938 which combined a set of grilles with a keyed columnar transposition. It was used for low level traffic and as a backup to Enigma; it is vulnerable to multiple anagramming.

043364 'Prinzipen des Datenschutzes und der Datensicherung'
M Wächter, *Datenschutz und Datensicherung (8/95) pp 465–470 (in German)*
Data protection laws can have the effect of forcing undesired and undesirable centralisation on organisations.

043365 'Sicherheit in Client/Server-Systemen'
G Weck, *Datenschutz und Datensicherung part 1: 3/95 pp 156–163; part 2: 4/95 pp 224–231; part 3: 5/95 pp 276–283 (in German)*
The author describes a number of the security problems which may arise when downsizing from a mainframe to client-server systems. He covers access control, authentication, end system security, network protection, and some of the features of systems such as Netware, NT and Unix.

043366 'EUROPOL-Konvention und Datenschutz'
T Weichert, *Datenschutz und Datensicherung (8/95) pp 450–458 (in German)*
Europol in the Hague is answerable only to the European commission; it deals with smugglers of drugs, stolen cars, nuclear material and human organs. It has escaped data protection rules because of its military nature, so for example it can collect national police data and pass this on to third parties outside Europe. This is in conflict with German institutional law; the democratic deficit in European institutions is particularly acute with such bodies, and the only restrictions on it are the sovereignty concerns of Britain and France.

043367 'Access al areas?'

L White, *Computer Weekly (28/9/95) p 42*

Vladimir Lenin has just been extradited from the UK to face charges of hacking into Citibank's corporate treasury management system in the USA. The victim has installed a one-time password system.

043368 'Bridging the gap'

M Whybrow, *Information Management and Computer Security v 3 no 1 (95) pp 4–6*

The Bishopsgate bomb showed that many London banks' disaster recovery plans were defective. A number of banks' and suppliers' arrangements are discussed.

043369 'Computer Security: For Fun and Profit'

HB Wolfe, *Computers and Security v 14 no 2 (95) pp 113–115*

The author argues that one should sell security in terms of expected loss reduction.

043370 'Fighting Mobile Phone Fraud — Who is Winning?'

K Wong, *Datenschutz und Datensicherung (6/95) pp 349–355*

Mobile phone fraud in Europe costs about £100m a year, and since it lets criminals place completely anonymous calls, it has attracted the attention of organised crime. The increased security of GSM phones has merely led villains to apply for SIMs in false names rather than using technical attacks.

043371 'Networking/Distributed Systems Security'

K Wong, *Datenschutz und Datensicherung (7/95) pp 407–417*

The author discusses the risks to distributed systems used for EDI, CAD/CAM, document image processing and facilities management.

043372 'The Culture of Control: Safeguarding Intellectual Property in the Age of Networks'

DR Worlock, *Network Security; part 1: June 95 pp 14–17; part 2: July 95 pp 13–17*

The author discusses encryption and its relation to IPR protection systems. It is already used by software and directory publishers, but a more comprehensive solution is held up by the lack of standards. Various possible models are discussed; desirable attributes for an object may include nonprintability, noncopyability, and nonsearchability. There are a number of initiatives including CITED (a European consortium), CUPID (a US one) and developments by CNRI, SMPTE and the UK Copyright Licensing Agency.

4 Formal Methods and Protocols

043401 'Practical and Secure Message Authentication'
S Bakhtiari, R Safavi-Naini, J Pieprzyk, *SAC 95 pp 55–68*

The authors propose a suite of authentication protocols based on MD5 with a secret key added in various ways including exclusive or'ing the key with the message rather than adding it as a prefix and/or suffix.

043402 'Seven More Myths of Formal Methods'
IEEE Software (July 95) pp 34–41

The authors cap Hall's seven myths of formal methods with seven more, which they seek to dispel: that formal methods delay development, lack tools, replace traditional engineering discipline, apply only to software, are unnecessary, are not supported, and are always used by formal methods people.

043403 'Towards a Classification of Key Agreement Protocols'
C Boyd, *CSFW 95 pp 38–43*

The author advises caution when selecting hash functions. His 'menagerie' of hash functions (acronyms, BOW and MIOW), help in classifying key agreement protocols into three different types. The basic idea is that hash functions may have to be noninvertible on more than one concatenated input in order for security results to be proved.

043404 'Access with Pseudonyms'
LD Chen, *CPAC 95 pp 542–555*

The author presents unforgeable, unlinkable pseudonyms which cannot however be abused by colluding users. It tackles the basic problem of pseudonymous credentials, namely that Alice could present Bob's blinded passport and ask authority to put in it a licence earned by Alice; this divertibility is prevented by running the zero-knowledge protocol twice.

043405 'Key Distribution without Individual Trusted Authentication Servers'
L Chen, D Gollmann, C Mitchell, *CSFW 95 pp 30–36*

The authors describe the problem of establishing secure (symmetric) channels between entities who share no secret, and where some authentication servers cannot be trusted. The advantages, over existing solutions, of their protocol, include, less (and smaller) messages, greater choice of hash function, and a lower computational complexity.

043406 'Key-spoofing attacks on nested signature blocks'
B Christianson, MR Low, *Electronics Letters v 31 no 13 (22/6/95) pp 1043–1044*

It may often be desirable to sign documents which themselves incorporate signatures. In this case, one must take care, since with many signature schemes one can find a bogus key which endows a chosen, bogus message with the same signature that the genuine message had under the genuine key. This can be used to attack mechanisms such as theft-proof capabilities, and to counter it the authors suggest that the CA's public key be incorporated in all key certificates.

043407 'Preserving Privacy in a Network of Mobile Computers'
DA Cooper, KP Birman, *Oakland 95 pp 26–38*

The authors tackled the problem of location security of mobile computers by developing a replicated memory service which allows users to read from memory without disclosing which locations they are reading, and without wasting too much bandwidth. Their solution uses a MIX-type network which bundles up read requests, and a store which uses secret sharing techniques to spread each word over a number of locations. Read and write protocols are described.

043408 'XCAPE: Implementing a Certification Authority'
J Dawes, *CPAC 95 pp 249–262*

The author describes a prototype certification authority based on X.509. The basic protocols are described. The difficulties encountered were with securing the online certificate generation process.

043409 'Automated Security Analysis of Cryptographic Protocols Using Coloured Petri Net Specifications'
E Doyle, SE Tavares, H Meijer, *SAC 95 pp 33–46*

The authors report the development of software to do automated state reachability analysis of crypto protocols using coloured Petri nets. It was exercised on a simple challenge-response protocols with a flaw that was found successfully, and then used on the CT2 and CT2+ protocols used to identify mobile telephone handsets in Canada.

043410 'Advances in public-key certificate standards'
W Ford, *ACM SIGSAC v 3 no 3 (July 95) pp 9–15*

The author discusses deficiencies which have been found in X.509 certificate formats, and the extensions being developed to cope with them. These include the need for more flexible naming (e.g., Internet addresses as well as X.509 names); policy information, especially where systems have no common root; key life cycle management; and techniques to limit the damage which can be done by a faulty or malicious certification authority.

043411 'Security Issues in a CDPD Wireless Network'
Y Frankel, A Herzberg, H Krawczyk, CA Kunzinger, M Yung, *IEEE Personal Communications v 2 no 4 (Aug 95) pp 16–27*

Cellular digital packet radio utilises excess bandwidth in the analog cellular phone system to provide new mobile services. Its authentication protocols are shown to be weak; active attacks are possible which steal users' identities or deny service to them. Alternative protocols are proposed, based on challenge response with keyed hash functions; optionally, Diffie-Hellman key exchange may be added to provide some anonymity over the air link.

043412 'The Design and Implementation of a Secure Auction Service'
MK Franklin, MK Reiter, *Oakland 95 pp 2–14*

The authors' Rampart system implements a trusted processor on a number of less trusted systems, using threshold signature and Byzantine agreement techniques, yet still provides a simple application programming interface which shields the system developer from the details. As a proof of this concept, they developed a distributed auction system which provides strong protection for both bidders and auctioneers, even if a fraction of the machines making up the auction service are subverted. Performance figures are given to support the practicality of the technique.

043413 'Secure Multiround Authentication Protocols'
C Gehrmann, *Eurocrypt 95 pp 158 - 167*

The author generalizes the multiround Gemmell-Naor authentication protocol and proves that for three rounds it is unconditionally secure for most practical message sizes, and easily implementable. The general case of multiround authentication protocols for an arbitrary odd number of rounds is also considered and shown to be secure.

043414 'Collisionful keyed hash functions with selectable collisions'
L Gong, *Information Processing Letters v 55 no 3 (11/8/95) pp 167–170*

The author discusses the use of hash functions with collisions to protect passwords against guessing attacks, and provides a new construction for them based on polynomial interpolation.

043415 'Optimal Authentication Protocols Resistant to Password Guessing Attacks'
L Gong, *CSFW 95 pp 24–29*

The author discusses a number of techniques for defeating password guessing attacks, by including nonces in logon protocols and otherwise. The threat model for such protocols may include insiders as well as outsiders. He exhibits a protocol which he claims is optimal.

043416 'Using Temporal Logic to Specify and Verify Cryptographic Protocols'
JW Gray, J McLean, *CSFW 95 pp 108–118*

The authors seek to provide a single logic in which requirements specification, protocol specification and proof of correctness can all be done within the same formalism. In this respect, they have effectively recast the Prolog, context free grammar and temporal logic components of the NRL protocol analyzer tool into Lamport's Raw Temporal Logic of Actions.

043417 'Password authentication without using a password table'
GB Horng, *Information Processing Letters v 55 no 5 (15/9/95) pp 247–250*

The author proposes a complicated scheme for the one-way encryption of passwords using RSA.

043418 'Two attacks on Neumann-Stubblebine authentication protocols'
TNL Hwang, NY Lee, CM Li, MY Ko, YH Chan, *Information Processing Letters v 53 no 2 (27/1/95) pp 103–108*

The authors point out attacks on two protocols by Neuman and Stubblebine, and propose an alternative variant.

043419 'Reasoning about Accountability in Protocols for ElectronicCommerce'
R Kailar, *Oakland 95 pp 236–250*

The author provides an authentication logic which, unlike BAN, does not express the notion of freshness. The idea is that many electronic commerce protocols depend on whether a transaction was ever authenticated, rather than on whether it was authenticated recently. He shows that this reduced apparatus is able to get useful results by finding two flaws: an Internet billing server proposal from Carnegie Mellon where accountability fails as transactions are encrypted before signature, and a protocol by Medvinsky and Neuman where it fails as a consequence of anonymity. He also verifies a delegation protocol from SPX.

043420 'An Efficient and Secure Authentication Protocol Using Uncertified Keys'
IL Kao, R Chow, *SAC 95 pp 47–54*

The authors propose a nonce-based authentication protocol, analyse it using the BAN logic, and discuss various options for preventing attacks based on the compromise of old session keys.

043421 'An Efficient and Secure Authentication Protocol Using Uncertified Keys'
IL Kao, R Chow, *Operating Systems Review v 29 no 3 (July 95) pp 14–21*

This is the journal version of the above.

043422 'Authenticate Yourself by Logon a Remote Password'
WB Lee, CC Chang, *CPAC 95 pp 149–162*

The authors propose a new authentication scheme in which Girault's zero knowledge scheme is used to prove knowledge of a password.

043423 'PCS Network Signaling Using SS7'
YB Lin, SK DeVries, *IEEE Personal Communications v 2 no 3 (June 95) pp 44–55*

The authors describe how SS7 signalling will be used in future PCS networks, how it will interface to the IS-41 authentication protocol suite, and the support provided for features such as handoff.

043424 'Several practical protocols for authenticated key exchange'
CH Lim, PJ Lee, *Information Processing Letters v 53 no 2 (27/1/95) pp 91–96*

The authors propose a number of key exchange protocols which fortify Diffie Hellman using symmetric or zero knowledge based authentication.

043425 'A Secure Smart Card Based Protocol for Electronic Data Interchange Messages'
M Looi, *CPAC 95 pp 421–432*

The author looks at various ways in which smart cards can be used to enhance Kerberos, such as by holding the password, holding tickets and keys, and even as a vehicle for transporting signing keys to partially-trusted terminals.

043426 'Formal methods, structured techniques, and security — A unified methodology'
A Lovering, *National Physical Laboratory Report DITC 235/95, June 95*

This report sets out to provide an 'off-the-shelf' methodology for building systems to be evaluated at the higher ITSEC levels. The feasibility, analysis and design stages are to be tackled with structured methods (SSADM and Yourdon are preferred) as well as security reviews (based on CRAMM); the analysis and design are to be tackled using formal methods such as Z/VDM/RAISE for information systems and RAISE for real-time systems.

043427 'An Augmentation of BAN-Like Logics'
W Mao, *CSFW 95 pp 44–56*

The author notes that errors are easily made during the protocol idealization step. His approach does not change the axioms of the logic, but proposes that stages of the idealization be described using new operators.

043428 'Methodical use of cryptographic transformations in authentication protocols'
W Mao, C Boyd, *IEE Proceedings on Computers and Digital Techniques v 142 no 4 (July 95) pp 272–278*

The authors discuss the various ways in which protocol security can interact with the choice of the underlying cryptographic algorithm. Presenting an opponent with a large amount of known plaintext can be a bad idea, and there are various ways to control this; it can also be dangerous to use decryption, because of the risk of oracle attacks, and one-way encryption is prudent where possible (as in many password and challenge response protocols). They discuss an attack on a protocol by Yahalom, and demonstrate a new cut-and-paste attack on one of the proposals of ISO CD 11770. Finally, they propose some new protocols.

043429 'Some New Key Agreement Protocols Providing Implicit Authentication'
AJ Menezes, MH Qu, SA Vanstone, *SAC 95 pp 22–32*

The authors describe active attacks on a number of key agreement protocols, most of which have the property of being vulnerable to the disclosure of old keys (as discussed by Burmester in **034604**). In the new attacks, manipulation of the protocol messages can induce incorrect beliefs about the binding of keys; for example, Alice and Bob might share a key but Alice might end up wrongly believing that the key was shared with the attacker, Charlie.

043430 'The Interrogator Model'
JK Millen, *Oakland 95 pp 251–260*

The author describes his protocol analysis tool, the Interrogator. It uses a state-transition model, just like the NRL protocol analyzer and Ina Jo, but uses a recursive search algorithm to look for flaws, and can now deal with the algebraic features often found in authentication protocols. Its evolution and message transformation model are described, and as an example the author shows how it finds the flaw in the Purdy-Simmons-Studier protocol. This flaw depends on the properties of exclusive-or and is thus beyond the reach of many purely symbolic tools.

043431 'On One-Pass Authenticated Key Establishment Schemes'
K Nyberg, *SAC 95 pp 2–8*

The author discusses how freshness can be integrated various key agreement schemes, most of the variants on authenticated Diffie-Hellman. Her paper includes details of an identity-based scheme proposed by France as an international standard, and on which an attack is shown.

043432 'Absorbing Covers and Intransitive Non-Interference'
S Pinsky, *Oakland 95 pp 102–113*

The author gives necessary and sufficient conditions for a system to satisfy intransitive non-interference, and develops a decision procedure for it. This problem is considered in the context of an encryption device with a bypass for header information; the goal is to show that interference with the ciphertext is limited to the crypto processor and the bypass channel. The solution uses a more complex purge function than standard noninterference does.

043433 'CSP and determinism in security modelling'
AW Roscoe, *Oakland 95 pp 114–127*

The author applies CSP to modelling a variety of confidentiality properties. Those which are based on determinism turn out to be more satisfactory, as they are preserved under refinement.

043434 'Modelling and verifying key-exchange protocols using CSP and FDR'
AW Roscoe, *CSFW 95 pp 98–107*

The author uses CSP to describe the agents in a protocol (responder, server, initiator, adversary) and uses the FDR tool to model check safety and liveness properties of the protocol. The use of process algebra forces one to pay close attention to exception handling.

043435 'Foiling Active Network Impersonation Attacks Made in Collusion With An Insider'
S Russell, *CPAC 95 pp 235–247*

The author discusses how firewall protocols may be used to screen electronic mail with a view to detecting insider attempts to collude in an outside attack.

043436 'Formal Methods in the Theta Kernel'
M Seager, D Guaspari, M Stilleman, C Marceau, *Oakland 95 pp 88–100*

The authors describe the role of formal methods in specifying and implementing a new kernel for a distributed multilevel operating system. They present their evaluation of a number of formal tools, including Larch, Larch/Ada, Penelope, Romulus and AdaWise. One problem turned out to be the Ada language itself; its lack of control over things like runtime scheduling means that covert channels cannot be controlled, and should limit systems written in it to B1.

043437 'Refinement and Extension of Encrypted Key Exchange'
M Steiner, G Tsudik, M Waidner, *Operating Systems Review v 29 no 3 (July 95) pp 22–30*

The authors discuss various attacks on the EKE protocol, such as when the compromise of an old session key is used to mount a dictionary attack on the password. They propose a 'minimal EKE' in which Alice sends Bob g^{N_A} encrypted using her password, Bob returns g^{N_B} both in clear and encrypted under the Diffie Hellman session key $g^{N_A N_B}$, and Alice replies with a one-way hash of g^{N_B} encrypted under this session key. They suggest that such a protocol can be implemented using a pool of impersonal, unregistered smartcards, from which users would select one at random when needed.

043438 'Recent-Secure Authentication: Enforcing Revocation in Distributed Systems'
SG Stubblebine, *Oakland 95 pp 224–235*

The author presents a formal language for reasoning about revocation and freshness. He discusses various approaches to the problem, such as certificate caches with exceptions, online certificate servers, and offline CAs with online revocation authorities. He presents as an alternative a freshness constrained revocation authority, which is described formally. The idea is to allow participants to tune authentication costs to risks on a per transaction basis.

043439 'On the Matsumoto and Imai's Human Identification Scheme'
CH Wang, T Hwang, JJ Tsai, *Eurocrypt 95 pp 382 -391*

A replay challenge attack on the Matsumoto-Imai scheme is described. In this a malicious terminal pretends to be the host and replays the challenges of the host to get the secret password. The authors propose a modified scheme which avoids this attack.

5 Secret Key Algorithms

043501 'Designing DES-Like Ciphers with Guaranteed Resistance to Differential and Linear Attacks'
CM Adams, *SAC 95 pp 125–130*

The author suggests fortifying block ciphers with a keyed nonlinear function such as multiplication just before each S-box lookup, as a means of frustrating differential and linear attacks.

043502 'Cocylcic Hadamard matrices over Z_t x Z_2^2'
A Baliga, KJ Haradam, *Australasian Journal of Combinatorics v 11 (Mar 95) pp 123–134*

The authors present a new uniform source of Hadamard matrices, namely the cocyles over the groups Z_t x Z_2^2 for t odd. This gives all the Williamson Hadamard matrices, and more besides.

043503 'A Fast Keyed Hash Function'
S Bakhtiari, R Safavi-Naini, J Pieprzyk, *CPAC 95 pp 205–221*

The authors present a new message authentication code primitive, called KHF, which is based on primitives of the type used in MD5. It is about half the speed of MD5.

043504 'DESV: A Latin Square Variation of DES'
G Carter, E Dawson, L Nielsen, *SAC 95 pp 144–158*

The authors propose replacing the XOR in DES with an arbitrary group operation defined by a Latin square, and give performance figures for different sizes of table. They discuss linear and differential attacks on this cipher, and claim that reduced numbers of rounds can be safely contemplated.

043505 'DES Variants More Resistant to Cryptanalytic Attack'
G Carter, E Dawson, L Nielsen, *CPAC 95 pp 445–457*

The authors propose two new DES variants. The first uses different keys in odd and even rounds, and can thus be used with those existing DES chips whose S-boxes are user loadable; the second combines the output of the round function with the other half block using a Latin square instead of exclusive or. Differential and linear analyses are given; the differential strength is only increased by a few bits in each case, but the linear strength can be improved substantially using the Latin square technique.

043506 'On the insecurity of arithmetic coding'
JG Cleary, SA Irvine, I Rinsma-Melchert, *Computers and Security v 14 no 2 (95) pp 167–180*

The Witten-Cleary proposal to encrypt data by prepending a secret string to a file and then compressing it using arithmetic coding is shown to be vulnerable to a very short chosen plaintext attack.

043507 'Signed groups, Sequences, and the Asymptotic Existence of Hadamard Matrices'
R Craigen, *Journal of Combinatorial Theory Series A v 71 no 2 (Aug 95) pp 241–254*

The author uses the theory of signed groups to prove the existence of Hadamard matrices of a number of new orders.

043508 'Multiple Encryption with Minimum Key'
IB Damgård, LR Knudsen, *CPAC 95 pp 435–444*

The authors propose stiffening triple encryption to make it more resistant to birthday attacks. The technique is that each data block will be DES encrypted with three keys, each of which is derived from two user supplied keys by double encryption of one of three fixed initial values.

043509 'Automated Reproduction of Plaintext Strings from their Combination'
E Dawson, L Nielsen, *CPAC 95 pp 185–201*

In world war two, a number of additive stream cipher systems were compromised by keystream reuse, resulting in a 'depth' which enabled the cipher to be solved provided that one could disentangle two plaintexts which had been exclusive or'ed together. In this paper, the authors describe a number of programs developed to recover such texts, and discuss the various tradeoffs between automated and manual analysis.

043510 'Latin Squares: Critical Sets and their Lower Bounds'
D Donovan, J Cooper, DJ Nott, J Seberry, *Ars Combinatoria v 39 (1995) pp 33–48*

A critical set is a uniquely completable part of a Latin square. The authors give a number of lower bounds on their size for various square orders, both in the general case and where the square represents a more ordered structure such as a group.

043511 'Pseudorandom Sequences Obtained from Expansions of Irrational Numbers'
H Ghodosi, C Charnes, J Pieprzyk, R Safavi-Naini, *CPAC 95 pp 165–175*

The authors suggest that the binary expansion of transcendental numbers such as x^y, where Y is an irrational algebraic number, might make good keystreams.

043512 'A Note on the Period of Interleaved and Decimated Sequences'
JD Golić, *CPAC 95 pp 177–184*

The author shows that, under uniform decimation, the period of a binary sequence may not decrease, and provided that the decimation coefficient is coprime to the sequence period it will remain the same.

043513 'Towards Fast Correlation Attacks on Irregularly Clocked Shift Registers'
JD Golić, *Eurocrypt 95 pp 248–262*

A shift register with linear feedback is clocked irregularly according to a decimated sequence, such as the shrinking generator. To reconstruct the polynomial, the optimal shrunk polynomial is found by statistical tests: search over low weights one at a time; look for multiples with the best match; then, statistically search for one tap at a time. To find the initial state with a known polynomial and unknown decimation sequence, the linear consistency test of Zeng, Yang, and Rao and probabilistic correlation attacks are applied. The attacks require a large amount of keystream and produce a feedback polynomial of high degree.

043514 'A Cryptanalysis of Clock-Controlled Shift Registers with Multiple Steps'
JD Golić, LJ O'Connor, *CPAC 95 pp 515–526*

Zivković's analysis of (0,1) clock controlled shift registers is generalised to the (0,d) case. This involves an exhaustive search of the initial state of the decimated register, and if this is r stages long the search requires $O(r2^{2^{d+2}})$ keystream, but there is nonetheless some relevant theory. The technique is to search the keystream for substrings which are either constant or alternating (0101...). The alternating string is the easiest one to embed, leading to the double exponential; it is conjectured that the actual length needed for most reconstructions is only exponential.

043515 'Discrete Optimisation and Fast Correlation Attacks'
JD Golić, M Salmasizadeh, A Clark, A Khodkar, E Dawson, *CPAC 95 pp 527–538*

The authors study the effects of fast correlation attacks of introducing techniques from discrete optimisation, namely fast resetting, subset selection and simulated annealing. With a sparse shift register of length 31, fast resetting increases the tolerable noise from 0.34 to 0.38; with the use of sliding windows and the other techniques too, this can be increased to 0.4.

043516 'Randomness Measures Related to Subset Occurrence'
HM Gustafson, EP Dawson, JD Golić, *CPAC 95 pp 299–310*

Standard series randomness tests which look for imbalance in the distribution of k-tuples, such as the poker test and Maurer's test, require about 5.2^k bits of keystream. The authors show that if one instead looks for collisions between k-tuples, then a comparable test can be done with only $2^{3+k/2}$ bits.

043517 'A one-key cryptosystem based on a finite nonlinear automaton'
M Gysin, *CPAC 95 pp 501–511*

The author presents a new block cipher. At alternate rounds, a Mealy machine whose core is a ten-input bent function is run backwards and forwards over the text.

043518 'A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-Up Lemma'
C Harpes, GG Kramer, JL Massey, *Eurocrypt 95 pp 24–38*

I/O sums (XORs of a function of the input and output of a round) are introduced to generalise Matsui's linear cryptanalysis attack; the average key imbalance is used as the measure the usefulness of an I/O sum. It is shown that a cipher can be secure against linear cryptanalysis but vulnerable to this attack, but no attacks on practical systems have been found.

043519 'Eigenvalues of Differential Transition Matrices'
P Hawkes, L O'Connor, *CPAC 95 pp 489–499*

The number of rounds required to thwart differential cryptanalysis depends on the second largest eigenvalue of the differential transition matrix, and in this paper the authors report experiments with random permutations to determine the expected size of this value for matrices defined by xor, modular addition and modular multiplication. For both 4-bit and 8-bit permutations, the eigenvalue was about one third larger for xor than it was for the modular operations; thus ciphers which use xor as a generic combiner (such as DES) should, ceteris paribus, be weaker than those which use modular operations.

043520 'A New Key Escrow Cryptosystem'
JM He, E Dawson, *CPAC 95 pp 83–101*

The authors argue that the US Escrowed Encryption Standard should have a longer LEAF in order to permit both a stronger checksum against LEAF forward search, the intended recipient's name, and a timestamp which could be used to prevent the FBI getting access to material encrypted either before or after the court order.

043521 'Avalanche Characteristics of Substitution-Permutation Encryption Networks'
HM Heys, SE Tavares, *IEEE Transactions on Computers v 44 no 9 (Sep 95) pp 1131–1139*

The authors show that the avalanche effect in SP-networks can be improved by doubling the S-box size, and investigate other aspects of diffusion such as the use of linear interround transformations and guaranteed avalanche. A guaranteed avalanche of order k means that a one bit input change will change at least k output bits; it was one of the DES design criteria that the S-boxes had a guaranteed avalanche of order 2.

043522 'A fast method for cryptanalysis of substitution ciphers'
T Jakobsen, *Cryptologia v XIX no 3 (July 95) pp 265–274*

The author presents an algorithm for solving substitution ciphers based on keyword guessing followed by hill climbing based on digram statistics. It uses matrix operations rather than manipulating the ciphertext directly, and its performance is tabulated for monoalphabetic through 5 alphabet substitutions.

043523 'Securing DES S-boxes against Three Robust Cryptanalysis'
KJ Kim, SJ Lee, SJ Park, DK Lee, *SAC 95 pp 131–143*

The authors present a set of replacement DES S-boxes chosen for improved immunity against differential. linear and Biham-Biryukov-Davies attacks. The basic idea is that the optimal characteristics should have eight boxes active in every other round. The resulting cipher is called s^5DES.

043524 'Large Periods of Nearly de Bruijn FCSR Sequences'
A Klapper, M Goresky, *Eurocrypt 95 pp 263–273*

Feedback with carry shift registers (FCSRs) are LFSRs with an additional memory bit, the carry. They are periodic, can be represented by 2-adic generating functions, and can be attacked with a 2-adic version of the Berlekamp-Massey algorithm. The goal is to find FCSRs with large period. To do this, the authors introduce l-sequences, which turn out to have nearly maximal period, be balanced, be as close to de Bruijn sequences as possible, and have excellent correlation properties.

043525 'Permuting matrices to avoid forbidden submatrices'
B Klinz, R Rudolf, GJ Woeginger, *Discrete Applied Mathematics v 60 no 1–3 (June 95) pp 223–248*

The problem of permuting a matrix so as to avoid generating a forbidden set of submatrices related to the forbidden subgraph problem and is shown to be NP-complete in general. Some known results in this field are surveyed.

043526 'New Hash Functions for Message Authentication'
H Krawczyk, *Eurocrypt 95 pp 301–310*

Toeplitz matrices generated by sequences with small biased distributions define hashing schemes which can be used for secure message authentication. As a special case one can use LFSR constructions, but the result extends to general families of sequences, several of which provide efficient close to optimal security.

043527 'On the Resistance of the CAST Encryption Algorithm to Differential Cryptanalysis'
J Lee, HM Heys, SE Tavares, *SAC 95 pp 101–114*

The authors argue that even with random S-boxes, CAST with ten rounds is more resistant to differential attacks than DES with 16. This uses probabilistic calculations on the distribution of input and output XORs.

043528 'A Low-Power CMOS Private Key Cipher for PCS Terminals'
AR McKinney, SE Tavares, *SAC 95 pp 159–171*

The authors describe the design of a block cipher based on a substitution permutation network which is optimised for low power consumption when implemented in an ASIC.

043529 'Explicit N-Polynomials of 2-Power Degree over Finite Fields'
H Meyn, *Designs, Codes and Cryptography v 6 no 2 (Sep 95) pp 107–116*

If $q \equiv 1 \pmod 4$ and f_1 is an irreducible monic self-reciprocal N-polynomial of degree 2 such that $F_1(1)f_1(-1)$ is a nonsquare in GF(q), then the polynomials f_n defined by $f_{n+1}(x) = (2x)^{2^n} f_n(\frac{x+x^{-1}}{2})$ are irreducible with linearly independent roots and trace compatible sequences.

043530 'Low Order Approximation of Cipher Functions'
W Millan, *CPAC 95 pp 311-325*

The author looks at how to get a quadratic approximation of a Boolean function supplied as a black box. He shows how to calculate the low order coefficients of the algebraic normal form of a function by evaluating it at a series of points. Tests show that this technique is consistently better than blind search techniques at finding a function with a minimum correlation value. He concludes that cipher functions should resist approximation by any low order Boolean function.

043531 'A Differential Cryptanalysis of Tree-Structured Substitution Permutation Networks'

L O'Connor, *IEEE Transactions on Computers v 44 no 9 (Sep 95) pp 1150–1152*

The author showed at Eurocrypt 93 that about 60% of the xor table entries of a random S-box are zero (**023525**). He uses this to show that if the SP-networks of Kam and Davida are constructed with random S-boxes, they have a differential strength of only $O(Rn/m)$ chosen texts, where there are R rounds, n bit blocks and m to m bit S-boxes.

043532 'An average case analysis of a differential attack on a class of SP-networks'

L O'Connor, *SAC 95 pp 115–124*

The author shows that the expected number of chosen plaintexts needed for a differential attack on a tree-structured substitution-permutation network is about linear in the number of S-boxes.

043533 'Convergence in Differential Distributions'

L O'Connor, *Eurocrypt 95 pp 13–23*

The author extends his Asiacrypt '94 work on odd round functions to model the distribution of differentials in 2-uniform mappings with a Markov chain. Assuming independent round keys, the rate of convergence of the transition matrix, as a measure of goodness, is shown to be exponential with high probability.

043534 'Adaptive Fuzzy Frequency Hopper'

PJ Pacini, B Kosko, *IEEE Transactions on Communications v 43 no 6 (6/95) pp 2111–2117*

The authors describe a system which uses fuzzy logic to adaptively generate a pseudorandom sequence for frequency hopping radio. It is trained on a sample pseudorandom sequence and is claimed to be harder to intercept than a traditional shift register sequence.

043535 'Software performance of encryption algorithms and hash functions'

B Preneel, *SAC 95 pp 84–93*

The author discusses the factors which contribute to the software speed of cryptographic primitives; these include the efficiency with which registers and cache can be utilised. He compares the performance of a number of block ciphers and hash functions on both Intel and Alpha processors.

043536 'On Weaknesses of Non-surjective Round Functions'

V Rijmen, B Preneel, *SAC 95 pp 94–100*

The authors point out that if a Feistel cipher's round function is not balanced, this could lead to a statistical attack. For example, six-round CAST with bent function S-boxes could in theory be broken with 82 known plaintexts (although the attack would require a table of size 2^{32}).

043537 'The Compression Function of MD2 is not Collision Free'

N Rogier, P Chauvaud, *SAC 95 pp 69–83*

The authors exhibit five collisions for the compression function of MD2. Their attack exploits various interbyte dependencies and its effect is that the security of MD2 depends entirely on the redundancy introduced by the checksum block.

043538 'A Coset Correlation for Sequences with Two-Valued Periodic Autocorrelation'

JJ Rushanan, *IEEE Transactions on Information Theory v 41 no 4 (July 95) pp 1150–1153*

The author generalises previous results on m-sequence coset correlation to any sequence with two-valued periodic autocorrelation which is constant on the cosets of an arbitrary Abelian group, an example being the sequences arising from difference sets.

043539 'Relating Nonlinearity to Propagation Characteristics'
J Seberry, XM Zhang, *CPAC 95 pp 283–297*

If p is the minimum dimension of the linear spaces of points at which a Boolean function on n variables does not satisfy the propagation criterion, then its nonlinearity is at least $2^{n-1} - 2^{n-p/2-1}$. If it satisifies the strict avalanche criterion, then its nonlinearity is at least 2^{n-2}, and this bound is tight.

043540 'An Infinite Class of Counterexamples to a Conjecture Concerning Nonlinear Resilient Functions'
DR Stinson, JL Massey, *Journal of Cryptology v 8 no 3 (summer 95) pp 167–173*

The construction of resilient functions from linear codes had led people to conjecture that if a resilient function of given parameters existed, then so did a linear function. However, the authors disprove this by constructing such functions from nonlinear codes.

043541 'The Concatentation and Partitioning of Linear Finite State Machines'
X Sun, E Kontopidi, M Serra, J Muzio, *International Journal of Electronics v 78 no 5 (May 95) pp 809–839*

The authors discuss the behaviour of concatenated linear finite state machines, and in particular linear feedback shift registers and linear cellular automata. Although the two are isomorphic in the case of irreducible characteristic polynomials, it turns out that reducible cellular automata have better partitioning and concatenation properties than reducible shift registers. Tables are given of all partitions up to length 16, all concatentations up to length 64 (and, in the case of low-cost machines, to 256).

043542 'Picking the Crypto Locks'
P Wayner, *Byte (Oct 95) pp 77 & 80*

The author provides a brief review of the last 10 years' advances in cryptanalysis and summarises which algorithms have yielded to which type of attack. He then mentions processor-in-memory architectures such as the proposed Cray 3 which could do keysearch tasks of the order of magnitude of DES under software control, and thus be configured for arbitrary block ciphers of comparable complexity.

043543 'Further Enumerating Boolean Functions of Cryptographic Significance'
YX Yang, BA Guo, *Journal of Cryptology v 8 no 3 (summer 95) pp 115–122*

The authors prove a number of counting theorems which relate the number of Boolean functions of a given size which satisfy various combinations of balance, nonlinearity, nondegeneracy, symmetry and uncorrelatedness.

043544 'On Nonlinear Resilient Functions'
XM Zhang, YL Zheng, *Eurocrypt 95 pp 274–288*

Resilient functions are constructed by a variety of methods. By examining both linear and nonlinear resilient functions, ones that simultaneously are highly nonlinear and have high algebraic degree were found.

6 Public Key Algorithms

043601 'Why You Can't Even Hope to Use Gröbner Bases in Public Key Cryptography: An Open Letter to a Scientist Who Failed and a Challenge to Those Who Have Not Yet Failed'
B Barkee, DC Can, J Ecks, T Moriarty, RF Ree, *Journal of Symbolic Computation v 18 no 6 (Dec 94) pp 497–501*

The authors argue that one cannot base a public key cryptosystem on the fact that Gröbner bases are hard to compute, since it would depend on the easier problem of deciding membership of an ideal. Having presented a 'typical' scheme, they outline an attack on it which uses the Buchberger algorithm, and challenge the community to come up with a stronger scheme, if one exists.

043602 'The Cryptanalysis of a Public-Key Implementation of Finite Group Mappings'
S Blackburn, S Murphy, J Stern, *Journal of Cryptology v 8 no 3 (summer 95) pp 157–166*

The Qu-Vanstone FGM public key cryptosystem is broken by showing that there are many equivalent private keys and providing an efficient way to find one of them. The attack throws doubt on all systems based on towers of subgroups.

043603 'Restrictive Blinding of Secret-Key Certificates'
S Brands, *Eurocrypt 95 pp 231 - 247*

A technique for designing efficient restrictive blind signature issuing protocols is described. This makes it possible for the receiver to blind the issued public key and the certificate but not a certain predicate of the secret key. The resulting protocol has three moves, is practical and can be proven secure with respect to a plausible intractability assumption.

043604 'A Class of Permutation Polynomial Vectors and Their Applications in Cryptography'
J Cazaran, *CPAC 95 pp 461–470*

RSA encryption can be generalised to Dickson polynomials, and the author examines whether any further generalisation is possible. She studies sets of permutation polynomials over an arbitrary finite ring which are closed under composition, and discusses how schemes such as RSA and Diffie-Hellman can be expressed in this context. However, no classes of polynomials are known other than the monomials and the Dickson polynomials whose composition is commutative.

043605 'On the Efficiency of Group Signatures Providing Information-Theoretic Anonymity'
L Chen, TP Pedersen, *Eurocrypt 95 pp 39–49*

The authors present a formal setting for group signatures and address the security issues involved. Bounds are obtained for the lengths of the secret keys and the auxiliary information of the designated group authority. These are optimal since they are met by a scheme of Chaum and van Heijst.

043606 'A New Identification Algorithm'
KF Chen, *CPAC 95 pp 557–562*

The author produces a new identification algorithm based on Gabidulin's rank distance code scheme.

043607 'Anonymous NIZK Proofs of Knowledge with Preprocessing'
S D'Amiano, G Di Crescenzo, *Eurocrypt 95, Rump Session, pp 413–417*

The authors present a non-interactive zero-knowledge proof with preprocessing which can be used to "fix" the cash scheme which they presented at Eurocrypt 94, and which is subject to the criticisms of Pfitzmann and others (**043624** below).

043608 'Securing Traceability of Ciphertext — Towards a Secure Software Key Escrow System'
Y Desmedt, *Eurocrypt 95 pp 147–157*

The security of Clipper is based on the fact that LEAFs which make the sender and receiver traceable cannot be removed from the ciphertext. This is achieved by using a tamperproof device. This article describes a novel approach based on Threshold Cryptography which does not require tamperproof devices. It uses the ElGamal scheme which is partitioned appropriately.

043609 'Verifiable Signature Sharing'
MK Franklin, MK Reiter, *Eurocrypt 95 pp 50–63*

With verifiable signature sharing, the holder of a signature (who might not be the original signer) can share it among n proxies in such a way that honest proxies can later reconstruct it, provided no more than a threshold of t proxies are dishonest (or faulty). Various settings are considered. For ElGamal type schemes the threshold is $t = (n-1)/3$, whereas for RSA type schemes $t = (n-1)/5$. Verifiable Signature Sharing has many applications such as cash key escrow and secure distributed auctions.

043610 'Public-key Cryptography on Smart Cards'
A Fuchsberger, D Gollmann, P Lothian, KG Paterson, A Sidiropoulos, *CPAC 95 pp 393–420*

This article surveys the state of the art in implementing public key techniques in smartcards. They then look at three smartcard applications - pay-TV, GSM and electronic wallets, discussing the Videocrypt and Mondex systems in particular. They caution against relying too much on the claimed tamper resistance of smart cards, and warn that system owners should prepare for regular changes of cards, keys and even algorithms.

043611 'Cryptanalysis of the blind signatures based on the discrete logarithm problem'
L Harn, *Electronics Letters v 31 no 14 (6/7/95) pp 1136*

The blind signatures proposed by Camenisch and others and by Horster and others are not truly blind; the signer can still identify them once the blinding has been removed.

043612 'Efficient sharing (broadcasting) of multiple secrets'
L Harn, *IEE Proceedings on Computers and Digital Techniques v 142 no 3 (May 95) pp 237–240*

The author presents a scheme based on DSS and polynomial interpolation which enables multiple secrets to be shared with a single shadow per user and a single public value per secret. It can cope efficiently with cheater detection and the broadcast of multiple secrets.

043613 'Comment - Digital signature with (t, n) shared verification based on discrete logarithms'
P Horster, M Michels, H Petersen, *Electronics Letters v 31 no 14 (6/7/95) p 1137*

The authors show how a signature scheme of Harn can be forged, and propose a fix.

043614 'Some Active Attacks on Fast Server-Aided Secret Computation Protocols for Modular Exponentiation'
SJ Hwang, CC Chang, WP Yang, *CPAC 95 pp 471–486*

The authors provide new active attacks on two server-aided signature schemes proposed by Kawamura and Shimbo in 1993.

043615 'Ripping Coins for a Fair Exchange'
M Jakobsson, *Eurocrypt 95 pp 220 - 230*

The notion of ripping coins is introduced and used to solve fair exchange problems in payment transactions. The idea is similar to paying for a future delivery with half a banknote, and handing over the other half on receipt of the goods. A general solution is given that can be used in any payment scheme which incorporates a challenge.

043616 'A Proposed Architecture for Trusted Third Party Services'
N Jefferies, C Mitchell, M Walker, *CPAC 95 pp 67–81*

The authors propose a new key escrow system, the aim of which is to permit users in different countries to exchange encrypted messages with the property that the authority in either the sender's or the receiver's country can decrypt any message he records. The idea is that each user will have a secret key x generated by its authority and a public key g^x; users X and Y will then use the key g^{xy} to communicate.

043617 'Fast RSA-type schemes based on singular cubic curves $y^2 + axy \equiv x^3 (\bmod n)$'
K Koyama, *Eurocrypt 95 pp 329 - 339*

An elliptic curve public key scheme is proposed which is claimed to be as secure as RSA and for which decryption is 2 times faster.

043618 'Low exponent attack against elliptic curve RSA'
K Kurosawa, K Okada, S Tsujii, *Information Processing Letters v 53 no 2 (27/1/95) pp 77–84*

In this journal version of **041619**, the authors set out their extension of Hastad's low exponent attack to the elliptic variants of RSA.

043619 'Cryptanalysis of Enhancing the Security of ElGamal's Signature Scheme'
CS Laih, WC Kuo, *CPAC 95 pp 137–141*

The authors provide an attack on a signature scheme of He and Kiesler (no. **033610**): given two valid signatures, a signature can then be forged for any message.

043620 'Authenticated encryption scheme without using a one way function'
WB Lee, CC Chang, *Electronics Letters v 31 no 19 (14/9/95) pp 1656–1657*

The authors propose a variant of the Horster-Michels-Petersen scheme (**022611**) which they claim does not require the use of a one way function.

043621 'Server-Aided Secret Key Exchange'
CH Lim, PJ Lee, *SAC 95 pp 9–21*

The authors propose server-aided protocols for Diffie-Hellman based authenticated key exchange. The server is basically used to precompute the confounders.

043622 'Server(Prover/Signer)-Aided Verification of Identity Proofs and Signatures'
CH Lim, PJ Lee, *Eurocrypt 95 pp 64 - 78*

Discrete log based identification and signature schemes are not suitable for verification using smart cards because of the asymmetric computational load between the prover/signer and the verifier. The authors present efficient and practical protocols for fast verification in which a verifier with limited computing power performs its computations with the aid of a powerful prover/signer.

043623 'Are Crypto-Accelerators Really Inevitable? 20 bit zero-knowledge in less than a second on simple 8-bit microcontrollers'
D Naccache, D M'raïhi, W Wolfowicz, A di Porto, *Eurocrypt 95 pp 404–409*

This article describes an efficient smart card prototype for zero-knowledge identification which uses an 8-bit processor. The efficiency is obtained by using a new technique for computing modular multiplications which is based (a) on an appropriate Chinese Remainder reduction of the modulus size to a suitable size for the controller, and (b) on Shamir's randomised multiplication. It is claimed that the overall complexity for the smart card is linear.

043624 'How to Break Another "Provably Secure" Payment System'
B Pfitzmann, M Schunter, M Waidner, *Eurocrypt 95 pp 121–132*

The scheme presented at Eurocrypt94 by S D'Amiano and G Di Crescenzo is flawed and does not provide untraceability. The authors analyze in great detail the subtleties of payment systems and point out the importance of a careful definition of the required security properties.

043625 'A New Identification Scheme Based on the Perceptrons Problem'
D Pointcheval, *Eurocrypt 95 pp 319 - 328*

The perceptrons problem is a new $\mathcal{NP}$-complete linear problem. Based on this the author considers various zero-knowledge identification protocols, and evaluates their security. These protocols are suited for smart card applications.

043626 'The quadratic and double quadratic residue ciphers'
F Rubin, *Cryptologia v XIX no 3 (July 95) pp 275–284*

The author proposes a variant of Blum-Blum-Shub which he claims is faster and more secure than RSA. The idea is to use two sequences of numbers generated by modular squaring, xor them together, and use all but the top 20 bits as a keystream sequence.

043627 'Relationship among the Computational Powers of Breaking Discrete Log Cryptosystems'
K Sakurai, H Shizuya, *Eurocrypt 95 pp 341–356*

The authors analyze the complexity of breaking various cryptosystems (Shamir's 3PASS, ElGamal, Bellare-Micali's non-interactive OT, Okamoto's conference key) which use a discrete logarithm setting, and compare it to the Diffie Hellman problem. In particular it is shown that for the certified discrete logarithm with prime modulus the complexities are equivalent.

043628 'A Public-Key Cryptosystem Utilizing Cyclotomic Fields'
R Scheidler, HC Williams, *Designs, Codes and Cryptography v 6 no 2 Sep 95) pp 117–131*

Rabin's scheme is provably as strong as factoring; if the encryption exponent is 2 or 3, then the equivocation in decryption is four and nine respectively. The authors show how this can be extended to arbitrary prime exponents, and give explicit algorithms for exponent 5. The complexities in the general case include the existence of units in the underlying cyclotomic field and the evaluation of higher power residue symbols by parties who cannot factor the modulus.

043629 'Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction'
CP Schnorr, HH Hörner, *Eurocrypt 95 pp 1–12*

By improving lattice reduction algorithms, the authors were able firstly to carry out a new and more powerful attack on Chor-Rivest, the last unbroken knapsack public key system, secondly to attack dimension 74 and 82 general knapsack problems, and finally to break many instances of Damgård's hash function. Their improvement on the L^3 basis reduction algorithm usually finds a shorter vector in the reduced basis. A heuristic based on the volume over the determinant of the lattice is used for the cutoff. They tried 50 Chor-Rivest problems, solved 21 the first time through, then 11 on the second pass, and 6 more on the third pass for 38 of 50. They also solved lattices of dimension 100 to 120 in about two hours on an Alpha.

043630 'Fair Blind Signatures'

M Stadler, J-M Piveteau, J Camenisch, *Eurocrypt 95 pp 209–219*

With fair blind signatures a trusted authority can deliver information which links the blinded signature to the message-signature. Two types are distinguished: in the first the information enables the signer to recognise the signed message, in the second to identify the sender. Several realisations are considered.

043631 'A cryptographic implementation for dynamic access control in a user hierarchy'

HM Tsai, CC Chang, *Computers and Security v 14 no 2 (95) pp 159–166*

The authors extend the Akl-Taylor scheme to allow users to change their keys.

043632 'Improved Digital Signature Suitable for Batch Verification'

SM Yen, SS Laih, *IEEE Transactions on Computers v 44 no 7 (July 95) pp 857–959*

The authors point out that the Schnorr scheme can be fairly easily adapted for batch verification of signatures; one has to stop various homomorphism based attacks, and this can be done by adding some randomness.

7 Computational Number Theory

043701 'Complete System of Two Addition Laws for Elliptic Curves'
W Bosma, HW Lenstra, *Journal of Number Theory v 53 no 2 (Aug 95) pp 229–240*

The authors show that the addition law for an elliptic curve can be expressed using homogeneous polynomials, thus avoiding the usual problem of dealing with a number of different cases for when one or more points are equal or zero.

043702 'On the primality of $n! \pm 1$ and $2.3.5 \cdots p \pm 1$'
CK Caldwell, *Mathematics of Computation v 64 no 210 (4/95) pp 889–890*

The author describes using a 486 PC with an L64240 arithmetic coprocessor (the successor of the Cruncher) to find fourteen new large primes, of which the largest was $3610! + 1$ at 11277 digits.

043703 'A $\lambda(p-1)$ Method of Factoring RSA's Modulus'
CY Chen, CC Chang, WP Yang, *CPAC 95 pp 225–231*

The authors propose an inefficient variant of Pollard's p-1 factoring method.

043704 'The twenty second Fermat number is composite'
R Crandell, J Doenias, C Norrie, J Young, *Mathematics of Computation v 64 no 210 (4/95) pp 863–868*

$2^{2^{22}}$ is composite. The authors describe how they proved this on an Amdahl mainframe and checked it using a number of workstations and a Cray.

043705 'On orders of optimal normal basis generators'
SH Gao, SA Vanstone, *Mathematics of Computation v 64 no 211 (7/95) pp 1227–1233*

The authors calculated some multiplicative orders of optimal normal basis generators for $GF(2^n)$ for $n < 1200$. They found a subclass of high order whose elements are very often primitive.

043706 'On the Number of Witnesses (a mod n) Providing a Proper Divisor of n'
H Gerlach, *Journal of Number Theory v 54 no 1 (Sep 95) pp 149–160*

Some of the bases a which witness to the compositeness of n using the Miller-Rabin test will provide a nontrivial factor of it of the form $\gcd(a^x - 1, n)$. The author shows that their number is of minimum order $4\sqrt{n}$.

043707 'Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems'
E Kaltofen, *Mathematics of Computation v 64 no 210 (4/95) pp 777–806*

The authors consider how Coppersmith's relation finding algorithm could be improved in fields larger than GF(2), and prove some running time results which hold for large enough fields.

043708 'Counting the number of points on elliptic curves over finite fields: strategies and performances'
R Lercier, F Morain, *Eurocrypt 95 pp 79 - 94*

Counting the number of points on elliptic curves over finite fields is needed for certain proposed cryptosystems and has recently become a lot easier, thanks to ideas of Schoof, Atkin, Elkies, Morain and Couveignes. The authors present some strategies based on their ideas, and describe an implementation which has been successfully tested up to $GF(2^{600})$ and $GF(2^{300} + 157)$. They anticipate significant further improvements.

043709 'Fast Generation of Prime Numbers and Secure Public-Key Cryptographic Parameters'
UM Maurer, *Journal of Cryptology v 8 no 3 (summer 95) pp 123–155*

The author discusses variants of the Miller-Wheeler method for generating large provable primes using Pocklington's lemma. He analyses the running times for generating provable versus probable primes, and concludes that the latter takes about a third longer.

043710 'A Block Lanczos Algorithm for finding Dependencies over GF(2)'
PL Montgomery, *Eurocrypt 95 pp 106 - 120*

Some integer factorization algorithms require several vectors in the null space of a large sparse binary $m \times n$ matrix, $m < n$. The author describes a variant of the Lanczos algorithm which applies a given matrix and its transpose to N independent binary vectors to produce a sequence of orthogonal subspaces of $\mathrm{GF}(2)^n$, each having dimension N. The algorithm requires $n/(N - 0.76)$ iterations. It was applied during the factorizations of 105-digit and 119-digit numbers using the general number field sieve and a 162-digit number using the special number field sieve.

043711 'An Implementation of the General Number Field Sieve to Compute Discrete Logarithms mod p'
D Weber, *Eurocrypt 95, pp 95 - 105*

It was long expected from theoretical considerations that the general number field sieve would give the fastest algorithm to compute the discrete logarithm modulo a prime. However, empirical data were lacking. In this article, the algorithm is reviewed and an implementation at the Universität des Saarlandes is described; this solved $23^x \equiv 29 \bmod p$ for a 40-digit prime p with 21 hours sieving. They also solved a number of smaller problems with both GNFS and Pohlig-Hellman; they suggest that the latter ceases to be competitive for quite small p ($> 10^{12}$.)

8 Theoretical Cryptology

043801 ‘Symposium on Computational Complexity and the Nature of Computer Science’
ACM Computing Surveys v 27 no 1 (Mar 95) pp 5–61
This article is made up of a number of short position papers on computation and complexity, with its star item being Juris Hartmannis’ Turing Award lecture.

043802 ‘Efficient Checkers for Number Theoretic Computations’
LM Adleman, MD Huang, K Kompella, *Information and Computation v 121 no 1 (15/8/95) pp 93–102*
The authors show how gcd and modular exponentiation algorithms can be checked; the former takes constant effort and the latter O(log n) additions and multiplications.

043803 ‘New Directions in the Theory of Identification via Channels’
R Ahlswede, Z Zhang, *IEEE Transactions on Information Theory v 41 no 4 (July 95) pp 1040–1050*
Unlike a normal channel, the capacity of a channel used for identification does change with feedback, and the authors give a coding theorem for this. They also consider the wiretap channel and show that the identification capacity is not lowered by eavesdropping, so long as one bit can be transmitted and identified correctly.

043804 ‘General Short Computational Secret Sharing Schemes’
P Béguin, A Cresti, *Eurocrypt 95 pp 194 - 208*
The authors extend Rabin’s information dispersal algorithms to general access structures and construct a computational scheme for such structures. They show that the size of the shares of each participant is nearly minimal.

043805 ‘A^2-codes from Universal Hash Classes’
J Bierbrauer, *Eurocrypt 95 pp 311–318*
Orthogonal arrays and universal hash codes are used to construct a new class of A^2-codes out of pairs of A-codes; these JK-systems are shown to be generalisations of previously known geometric constructions. Properties about the size of the new codes are proved, and new universal hash codes are constructed as well.

043806 ‘A note on dynamic threshold schemes’
C Blundo, *Information Processing Letters v 55 no 4 (25/8/95) pp 189–193*
Dynamic threshold schemes allow a quorum of participants, each of whom has seen one of a set of broadcast messages, to reconstruct a secret, while less than the quorum has no information even after seeing all these messages. Tight lower bounds are provided on the size of the participants’ information and of the messages; a construction is given which attains them.

043807 ‘Quantum Oblivious Mutual Identification’
C Crépeau, L Salvail, *Eurocrypt 95 pp 133–146*
A simple and efficient protocol for mutual identification based on the exchange of quantum information is presented. It allows honest parties to check mutual ownership of a secret string, while a dishonest party would have to enter the protocol exponentially many times to get nonnegligible information.

043808 ‘Zero-Knowledge Arguments and Public-Key Cryptography’
A De Santis, G Di Crescenzo, G Persiano, *Information and Computation v 121 no 1 (15/8/95) pp 23–40*
The authors show that using a short public random string along with Diffie Hellmann allows non-interactive implementation of oblivious transfer without a trusted centre, and of non-interactive perfect zero-knowledge arguments for all languages in NP.

043809 'Recycling Random Bits in Composed Perfect Zero-Knowledge'
G Di Crescenzo, *Eurocrypt 95 pp 367–381*

For non-interactive perfect zero-knowledge proofs, the same number of public random bits suffices to prove that one out of polynomially many statements is true as to prove a single statement. For interactive perfect zero-knowledge proofs, polynomially many statements may be proved with only a constant times as many random bits as needed to prove a single statement. In effect, bits from the first proof are re-used in the second, and so on.

043810 'Anonymous wireless rings'
K Diks, E Kranakis, A Malinowski, A Pelc, *Theoretical Computer Science v 145 (10/7/95) pp 95–109*

The authors introduce anonymous wireless rings; each processor has a single buffer, and cannot tell which of its neighbours the arriving bit has come from. This increases anonymity over the conventional wired ring, but turns out to be computationally equivalent, both in terms of the kind of functions which can be computed and the bit complexity of input collection. A suite of bit collection algorithms is presented for both synchronous and asynchronous operation. Open problems include symmetry breaking and leader election.

043812 'Key Distribution Patterns and Secret Sharing Schemes'
D Donovan, *CPAC 95 pp 369–380*

The author investigates the relationship between secret sharing schemes and key distribution patterns, and discusses the circumstances under which the set of nodes which must collude in order to compromise the set of subkeys shared by two parties is bounded below.

043813 'Amortized Communication Complexity'
T Feder, E Kushilevitz, M Naor, N Nisan, *SIAM Journal of Computing v 24 no 4 (Aug 95) pp 736–750*

The authors define the amortized communication complexity of a function on a number of Boolean variables as $1/m$ times (the complexity of computing m separate instances of it). They give examples of functions for which this is either much more or much less than the normal communications complexity.

043814 'Verifiable Secret Sharing as Secure Computation'
R Gennaro, S Micali, *Eurocrypt 95 pp 168 - 182*

A new definition of verifiable secret sharing is proposed and a practical protocol implementing it is given. It is shown that this definition is preferable to earlier ones. Applications in the field of secure multiparty computation are provided.

043815 'How to Fairly Reconstruct a Shared Secret'
JM He, E Dawson, *CPAC 95 pp 381–390*

Verifiable secret sharing does not completely solve the problem of cheaters; in a typical VSS scheme, the cheater can be detected, but he can also end up in sole possession of the shared secret. The authors therefore look at ways in which prevention can be added to detection; the solution they propose is to share the secret bit by bit using a VSS scheme. They provide bounds on the rate at which information is leaked by such an arrangement.

043816 'Efficient Secret Sharing Without a Mutually Trusted Authority'
WA Jackson, KM Martin, CM O'Keefe, *Eurocrypt 95 pp 183 - 193*

The authors address the problem of establishing a secret sharing scheme without the use of a mutually trusted authority for the generation and distribution of the shares. A general protocol is discussed and its efficiency is considered.

043817 'Cryptographic Lower Bounds for Learnability of Boolean Functions on the Uniform Distribution'
M Kharitonov, *Journal of Computer and System Sciences v 50 no 3 (June 95) pp 600–610*

If the n by $n^{1+\epsilon}$ subset sum problem were hard, then a pseudorandom function generator could be constructed from shallow Boolean functions, and this would mean that circuit learning was hard.

043818 'Combinatorial Bounds for Authentication Codes with Arbitration'
K Kurosawa, T Obana, *Eurocrypt 95 pp 289–300*

Digital signatures are only computationally secure, and authentication codes cannot provide non-repudiation. Thus, Simmons introduced authentication codes with arbitration. Only entropy-based error bounds for these codes were known until this work calculated combinatorial lower bounds for the various cases of cheating. The bounds are proved to be tight.

043819 'Fair reconstruction of a secret'
NY Lim, L Harn, *Information Processing Letters v 55 no 1 (7/7/95) pp 45–48*

The authors propose to stop cheating during secret reconstruction by giving each participant extra information — including a certificate for his shadow — to enable mutual verification of shadows as they are disclosed.

043820 'Universal Hash Functions & Hard Core Bits'
M Näslund, *Eurocrypt 95 pp 356 - 366*

The bit security of two types of universal hash functions is considered: linear functions over GF(2) and linear functions over GF(p), p prime. For the first we have individual security for all bits, for the second for the $O(\log n)$ least significant bits. Both have $O(\log n)$ simultaneously secure bits.

043821 'A coding theoretic approach to extending designs'
GT Kennedy, V Pless, *Discrete Mathematics v 142 (July 95) pp 155–168*

If the words of weight $n-1$ and $n+1$ in a binary $(2n, n, d)$ code (with n odd) hold complementary t-designs, then the vectors of weight n in a coset of weight 1 also hold a t-design, which can be extended. Designs in cosets of self-dual codes are also studied.

043822 'Receipt-Free Mix-Type Voting Scheme — A practical solution to the implementation of a voting booth'
K Sako, J Kilian, *Eurocrypt 95 pp 393 - 403*

A receipt-free voting scheme is proposed in which the only physical assumption made is the existence of a private channel through which the center can send a message to each voter.

043823 'On the Information Rate of Perfect Secret Sharing Schemes'
M van Dijk, *Designs, Codes and Cryptography v 6 no 2 (Sep 95) pp 143–169*

The author studies the optimal average rate of perfect secret sharing schemes based on connected graphs on six vertices. He shows how to construct graphs of maximum degree (up to 3) whose rate is arbitrarily close to Stinson's lower bound.

043824 'A geometric approach to sharing secrets'
TC Wu, WM He, *Computers and Security v 14 no 2 (95) pp 135–145*

The authors remark that geometric threshold schemes can be constructed using quadratic instead of linear varieties.

9 Book Reviews

'CRYPTOGRAPHY — THEORY AND PRACTICE'
Douglas R Stinson
CRC Press Inc., 1995, ISBN 0-8493-8521-0

Doug Stinson's textbook is based on graduate lectures in cryptology which he gives at the University of Nebraska, and so is written as a mathematics textbook rather than an engineering one — there is little of significance on applications. Its goal is rather to get the reader to the point where she can understand many of the papers presented at recent Crypto conferences.

It goes through the usual basics such as substitution ciphers, Shannon's theory and number theory, and there is an exceptionally good section of differential cryptanalysis which presents worked examples of attacks on 3-round and 6-round DES; this will be most helpful to the many workers who still struggle with some of the details of this technique.

There is a lot of public key mechanics, and a chapter each on A-codes, secret sharing, pseudorandom generators (of the Blum-Blum-Shub type) and zero knowledge. Again, these provide a welcome and overdue introduction to active areas of research, and could save young researchers the considerable effort of reverse engineering the state of the art from the literature.

The book's weak points, like its strong points, reflect the differences between US and European academic cryptography. There is next to nothing on stream ciphers or authentication protocols, and this reviewer (being European) finds it strange that such an otherwise complete book fails to mention either the Meier Staffelbach results or the BAN logic. We hope that the author will remedy these deficiencies in the second edition, for his book is a good one.

'ALGEBRAIC CODED CRYPTOSYSTEMS'
John Keith Gibson
Royal Holloway and Bedford New College, University of London, 1995

Keith Gibson's thesis is about his attacks on variants of the McEliece cryptosystem. The starting point was a proposal by Gabidulin to use rank distance codes instead of Goppa codes, and a claim that this construction allowed a more efficient system. Gibson's first attack (see **042605**) showed that larger parameters would have to be chosen, thus eliminating the claimed advantage in performance.

Gabidulin responded with a modified version, which he proposed at Cirencester 93 (see **041611**). An attack is presented on this as well, and a number of tricks developed to implement the attacks quickly are described; software is provided on a diskette. There are also results on Goppa codes, one of which implies that the McEliece cryptosystem has many equivalent trapdoors, rather than the single one which had previously been thought. This issue of the number of secret keys may be of broader interest, as it has its counterpoint in public key cryptosystems based on towers of subgroups and even in the key spoofing attacks on systems such as RSA.

'SMART CARDS'
José Luis Zoreda, José Manuel Otón
Artech House, 1994; ISBN 0-89006-687-6

The authors provide a thorough introduction to smart card technology. They cover the history, hardware, standards, and applications; they go into some detail on instruction sets, interface conventions, communications protocols and those aspects of smart card operating systems (such as hierarchical file structures) which are (or might be) covered by standards such as ISO 7618.

They then describe a (fictitious) card conforming to ISO 7618 and use it to show how one might go about programming a smart card. They include C source code for a number of sample software modules to illustrate how keys might be managed, and then go into detail about personalisation and diversification. Next they discuss applications in banking, healthcare, education, the administration of welfare benefits and agricultural quotas, prepaid meters and the certification of gold coins held for investment. They end up with a chapter on possible future applications ranging from biometrics through transport and electronic cash.

'ROBERT SLADE'S GUIDE TO COMPUTER VIRUSES'
R Slade
Springer-Verlag, 1994; ISBN 0-387-94311-0

The author provides a thorough introduction to computer viruses at a fairly non-technical level. Over half of the book is given over to technical assessments of antiviral products and reviews of several dozen books on viruses and related subjects. There is also an extensive list of industry contacts. The main market for this book is not the research community, but the working IS manager responsible for an organisation's PCs; for this community, it is likely to be more useful than the more scientific treatises such as Cohen's, and even researchers may find its engineering detail and pragmatic point of view to be stimulating.

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 1996 (volume 4) plus a set of the remaining back numbers (currently v 2 no 1, 3 and 4 and all of v 3) at a price of £90 for individual subscribers and £145 for corporate subscribers. Electronic copies of back numbers a year and more old may be fetched from `http://www.cl.cam.ac.uk/users/rja14`.

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: ....

We can accept email credit card orders, but some card issuers insist that your card number and expiry date be encrypted. You can use PGP; a key with fingerprint `E5C7 93BE 379D 2842 49DC A809 A147 05F6` can be fetched from `http://www.cl.cam.ac.uk/users/rja14`. You can also 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