Computer and Communications
Security Reviews

Volume 4 Number 1 (March 1995) ISSN 1352-6278

CONTENTS

Applications and Engineering	3
Operating System and Database Security	13
Security Management and Policy	19
Formal Methods and Protocols	26
Secret Key Algorithms	31
Public Key Algorithms	38
Computational Number Theory	43
Theoretical Cryptology	45
Book Reviews	48

Editor: Ross Anderson *Cambridge*

Contributing Editors:

Mike Burmester *London*
Tom Cusick *Buffalo*
Jeremy Epstein *Cordant*
Dieter Gollmann *London*
Richard Graveman *Bellcore*
Sushil Jajodia *George Mason*
Kwok-Yan Lam *Singapore*
Ira Moskowitz *US Naval Labs*
Bart Preneel *Leuven*
Rei Safavi-Naini *Wollongong*
Pierangela Samarati *Milan*
Bruce Schneier *Counterpane*

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 28 February 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:

Cirencester 93: Fourth IMA Conference on Cryptography and Coding, 13–15 December 1993; *proceedings published by the IMA, Feb 1995, ISBN*

ANTS 94: First International Symposium on Algorithmic Number Theory, May 1994, Ithaca, NY; *proceedings published as Springer LNCS v 877*

Info Theory 94: IEEE-IMS Workshop on Information Theory and Statistics, 27–29 October 1994, Alexandria, Virginia, USA; *proceedings published by the IEEE press*

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

Cardis 94: First smart card research and advanced applications conference, 24–26 October, Lille, France; *proceedings published by the University of Lille*

ISITA 94: International Symposium on Information Theory and Its Application 1994

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

Fairfax 94: Second ACM Conference on Computer and Communications Security, 2–4 November 1994, Fairfax, Virginia: *proceedings published by the ACM ISBN 0-89791-732-4*

Asiacrypt 94: Fourth Workshop on the Theory and Applications of Cryptology, 28 November – 1 December 1994, Wollongong, Australia; *page numbers from preproceedings*

JW-ISC 95: 1995 Japan-Korea Joint Workshop on Information Security and Cryptology, 24-27 January 1995, Inuyam, Aichi, Japan

Some of the articles in ANTS were reviewed in v 3 no 3, and some of those in both NCSC and ESORICS were covered in v 3 no 4.

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

1 Applications and Engineering

041101 'Higher Radix Nonrestoring Modular Multiplication Algorithm and Public-Key LSI Architecture with Limited Hardware Resources'
M Abe, H Morita, *Asiacrypt 94 pp 307–317*

The authors present a design for a modular exponentiation chip which uses higher radix arithmetic and a RAM based architecture. With 13,000 gates and six 512 bit RAMs, a 512 bit exponentiation should take a tenth of a second at 17MHz.

041102 'The Radar Concept using Neural Networks'
T Alexandre, *Cardis 94 pp 15–31*

The author describes a prototype system for monitoring spending patterns, which uses neural network techniques and whose runtime code can be fielded in a smartcard and will generate an alarm if the card is used to make an unusual transaction.

041103 'Making Smartcard Systems Robust'
RJ Anderson, *Cardis 94 pp 1–14*

The author discusses the nature of security robustness, and argues that explicitness rather than overdesign or redundancy should be the organising principle. Above all, one must make the system goals and threat model explicit; but the principle is also useful in enforcing the security properties of the implementation. A distributed TCB, such as one gets with smartcard based payment systems, can make explicit checking of security relevant data items both mandatory and pervasive. This was implemented in a smartcard payment system now fielded in a number of countries.

041104 'Whither Cryptography?'
RJ Anderson, *Information Management and Computer Security v 2 no 5 (1994) pp 13–20*

Three widely held beliefs on cryptography are that it is mostly used to keep communications secure, that it is the only way to secure electronic evidence, and that most attacks on cryptosystems involve technical skill. These are shown to be mistaken. A survey of applications reveals that most applications are concerned with preventing fraud, in ATMs, telephone cards, pay-per-view TV decoders, burglar alarms and the like. Furthermore, cryptographic evidence can usually be defeated in court by aggressive discovery techniques, and most failures result from the opportunistic exploitation of design or operational blunders rather than from technical attacks.

041105 'Apacs sets standards for cheques'
D Austin, *Banking Technology (Mar 95) p 9*

Advances in printing technology have enabled a large number of unsupervised commercial printers to enter the bespoke corporate cheque market, leading to a rise in cheque fraud. The UK banks are now trying to impose standards and accreditation.

041106 'Smart times ahead'
D Austin, *Banking Technology (Feb 95) pp 22–25*

The case for smartcards in banking was always hard to make on security alone, but the growth of card forgery may be changing this. Of equal importance may be the ability to offer space to retailers for incentive schemes, and to gather information about customer spending patterns.

041107 'Optical extra for mag-strip cards'
Banking Technology (Mar 95) p 49

This article describes a new security technology, which is based on an optical hologram containing a unique sequence number and printed on a magnetic card. It is claimed to be cheaper and harder to forge than a smartcard chip.

041108 'Telephone Cards and Technology Development as Experienced by GPT Telephone Systems'

PJ Bass, *GEC Review v 10 no 1 (95) pp 14–19*

This article surveys world trends in telephone payment card technology. By the end of the decade, smartcards are expected to predominate, with 100-150 countries using them, the driving force behind this is the network costs involved in validating more easily forgeable tokens online.

041109 'Hole in the wallet'

F Booth, *Banking Technology (Dec 94/Jan 95) pp 18–22*

This article provides an overview of business pressures on cash dispenser networks in Europe. It discusses per-ATM profitability, cash handling costs, and various aspects of strategy.

041110 'VISA hits fraud with cards'

Cards International (21/12/94) p 4

VISA's cardholder risk identification system (CRIS) is a neural network database which spots high risk transactions. It is being piloted in Spain because of the high levels of fraud there with foreign credit cards.

041111 'Junk mail underscores privacy concerns, says MC'

Cards International (22/2/95) p 6

Mastercard has suggested that its member banks buy customer consent to be on junk mailing lists using incentives such as lower charges. The idea is to defuse the privacy debate and forestall legislation.

041112 'Chip: how secure, how soon and how much?'

Card World International (Feb 95) p 4

This article discusses the Europay-VISA-Mastercard smartcard initiative. The key will be key to the spread of the technology, and should enable more advanced offering such as an electronic cash system being developed by Digicash and Mastercard, which will make public key technology available at $1 a card.

041113 'Bank-backed EP tipped as Dutch success story'

Card World International (Dec 94 — Jan 95) p 4

There are now three electronic purse projects competing for business in the Netherlands. Interpay, owned by the banks, will provide cards holding a few hundred guilders; Primeur card, backed by the retail chains, is already rolling out and provides space for store incentive programmes; and the PTT card is expanding from phone calls to parking and public transport. Unfortunately, these cards are not likely to be compatible.

041114 'EP answers a banking prayer'

Card World International (Feb 95) p 5

This article describes a project to introduce smartcard based electronic purses in Zambia and a number of other African countries, where banking is otherwise stuck in the 1950's by the lack of infrastructure. The protocol is customer card to merchant card, and lost customer cards can be replaced with the balance intact.

041115 'German A555 takes its toll'

Card World International (Dec 94 — Jan 95) p 6

Nine players are involved in road toll pilots in Germany, and some of the technologies are described; they include both smartcard and tag, beacons and GPS/GSM, anonymous and registered, and offline and online systems. A choice of technology should be made this year for implementation in 1998.

041116 'Moneta set to take country by storm'

Card World International (Oct 94) p 3

An Italian electronic purse system hopes to benefit from the tax regime, in that by combining debit and credit card functions it can put all transactions on one statement and thus save enough tax (and postage) to pay the card fee. However, high merchant fees remain a problem for Italy's many small shopkeepers and so there is a facility for the customer to pay the fee.

041117 'Proton pilots set EP scene in Belgium'
Card World International (Dec 94 — Jan 95) p 5

Belgium's electronic purse, Proton, is described. It is aimed at newsagents, taxis, vending machines, car parks and public transport; the cards can be recharged at ATMs, but person-to-person transactions are not allowed.

041118 'A new generation of terrestrial and satellite microwave communication products for military networks'
M Darman, E le Roux, *Electrical Communication (Q4 94) pp 359–364*

This article describes a family of secure tactical radios manufactured by Alcatel which support a number of features to prevent eavesdropping, jamming and the abuse of captured equipment. These include encryption (of both signal and control information), spread spectrum and remote control.

041119 'A Fast (and Secure) Track to Hypertext'
Data Communications International (Jan 95) pp 112–113

This article describes the Netscape browser products with enhanced security, based on RSA and a proprietary protocol called Secure Sockets Layer.

041120 'Physiognomic access control'
H Davies, *Information Security Monitor v 10 no 3 (Feb 95) pp 5–8*

The author describes an access control system developed at Cardiff University. At logon, the user is presented with nine faces, three of which are known to him, and he must click on these correctly.

041121 'Intrusion Protection for Networks'
JB Dawson, *Byte (April 95) pp 171–2*

This article reviews a firewall product which filters IP packets according to user-defined rules and supports a scripting language.

041122 'SCALPS'
JF Dhem, JJ Quisquater, D Veithen, *Cardis 94 pp 119–131*

The authors describe the fabrication of a smartcard chip in 1.5μ CMOS with a surface area of 11.8mm^2 which can perform 33 512-bit modular multiplications per second. Is is intended for use in smartcards with the Guillou-Quisquater scheme, with a view to low value payment applications.

041123 'EDI Security'
T Dosdale, *Financial Technology Insight (Nov 94) pp 5–10*

The author looks at the EDIFACT security framework and related standards; he also describes test implementations and likely costs.

041124 'A Universal Memory Card Server'
P Durant, P Ardouin, MJ Papillon, A Gamache, G Lavoie, J Bérube, JP Fortin, *Cardis 94 pp 133–139*

The authors describe a security server developed for use with smartcards in a portable medical record project in Rimouski, a town of 35,000 inhabitants in Quebec. The various security management requirements are described; they are similar to those in a conventional database system.

041125 'Latest thinking in fraud prevention and computer security for financial institutions'

J Essinger, *Financial Technology Insight (Dec 94) pp 12–14*

The author describes some of the security measures which banks ought to take to cut down ATM fraud.

041126 'Smart Cards From There to Here — part 1'

DB Everett, *Smart Card News v 4 no 2 (Feb 95) pp 36–39*

This introduction to smartcards starts with the basic physical and electrical interface specifications and a description of the main kinds of chip used.

041127 'Australia to test electronic cash'

Financial Technology International Bulletin (Jan 95) p 7

A pilot ecash scheme is being run in Newcastle, New South Wales, in the second half of 1996. Some 50,000 cards will be issued, and recharged at ATMs.

041128 'Card firms react to cybercash threat'

Financial Technology International Bulletin (Feb 95) pp 1 & 12

Established credit card groups' main reaction to electronic cash on the Internet is to build alliances — Mastercard with Netscape and VISA with Microsoft.

041129 'Crest deadlines in double jeopardy'

Financial Technology International Bulletin (Feb 95) p 2

The UK equity settlement system, Crest, has had problems with its two network suppliers, particularly over security requirements. However it is unwilling to jettison one or both of them because of the delays this would cause.

041130 'NatWest to participate in consumer trials of interactive home banking'

Financial Technology International Bulletin (Dec 94) pp 6–8

A large UK bank is participating in a trial of video-on-demand and home shopping technology in Ipswich. They may eventually bundle this with Mondex as a delivery system.

041131 'Citibank: heading anti-fraud initiatives'

Fraud Watch (Winter 94) pp 6–7

Citibank's Asian losses from card counterfeiting have dropped 80–90% since 1991. The strategy ws to stop relying on merchants; visual card checks were replaced with CVVs checked by online POS terminals. Floor limits were set to zero and cards were delivered by courier.

041132 'Lobby bank attack'

Fraud Watch (Winter 94) pp 6–7

All big four UK banks have been cheated by villains installing bogus card readers and PIN pads on the doors of their electronic banking lobbies, often overnight.

041133 'American Express heads for cyberspace'

JA Giannone, *Cards International (8/2/95) p 6*

Amex has opened a facility on America Online to enable its customers to make enquiries, and to cross-sell travel and catalogue services. Its strategy is to get into the market quickly rather than trying to control the distribution channel.

041134 'Intelligent systems becoming smarter as they evolve'

S Goonatilake, *Fraud Watch (Winter 94) p 4*

The success of neural nets in detecting credit card fraud has prompted a lot of further development work. The London Stock Exchange is building a system to detect insider dealing; a US firm is tackling bogus healthcare claims; and an increasing amount of work is being done with genetic algorithms, which are seen as a more transparent way of getting the same results.

041135 'A computer package for measuring the strength of encryption algorithms'
H Gustafson, E Dawson, L Nielsen, W Caelli, *Computers and Security v 13 no 8 (94) pp 687–697*

The authors describe a set of three software packages which do the standard statistical tests on encryption algorithms, and look at correlations, propagation and sequence complexity.

041136 'Distributed Database Security'
D Harris, D Sidwell, *Computers and Security v 13 no 7 (94) pp 547–557*

The authors describe the security features of Oracle release 7.1. It has a logon protocol similar to Kerberos and supports various distributed authentication services, such as OSF DCE, and software encryption of data on the network using DES or RC4. The basic version is evaluated to C2, and a B1 multilevel secure version is also available.

041137 'Countering the bomb threat'
RW Ince, *Computer Audit Update (Jan 95) pp 3–12*

The author describes a tool called BombCAD, which simulates explosions in or near buildings and thus lets architects and engineers minimise the risk.

041138 'Intelligent tags — a review of current and emerging technologies'
P Hawkes, *Smart Card News v 3 no 12 (Dec 94) pp 237–8 (part 1); v 4 no 1 (Jan 95) pp 16-18 (part 2)*

Intelligent tags come from two evolutionary streams — radio tags and smart cards. These are now converging, and a number of protocols and products are described.

041139 'Australian Banking: Cheque Charges Versus Cheque Fraud'
RC Holland, *Journal of Security Administration v 17 no 2 (Dec 94) pp 21–31*

Australia suffers a relatively high level of cheque fraud. There are many direct causes, such as poor uptake of references on new customers, but the central reason may be that, unlike with credit cards, the banks carry no liability — indeed, they charge a fee for every cheque which bounces.

041140 'Security enhanced architecture of real-time satellite simulator'
KY Hong, WS Choi, JY Kang, HJ Lee, DK Kim, *JW-ISC 95 pp 219–227*

The authors describe the security-enhanced architecture of Advanced Real-Time Satellite Simulator (ARTSS), developed to support the telemetry, tracking, and command operations of the Korean ETRI satellite control system.

041141 'Banks ponder Internet payments'
D Jones, *Banking World (Jan 95) p 39*

A UK bank has finally acquired a web address, but worries about security have so far prevented any payment service being offered.

041142 'Must there be a Euro ACH?'
D Jones, *Banking World (Mar 95) p 41*

The prospect of European monetary union is preventing the establishment of a European clearing house for financial transactions. Meanwhile, various banks have established proprietary systems.

041143 'The electronic detective'
D Jones, *Banking World (Feb 95) p 24*

VISA's antifraud measures are briefly described. They include collecting and disseminating information on high risk merchants and fraud patterns, and an experimental intrusion detection software system which generates alarms at transactions which look risky.

041144 'Exchange of Patient Records — Prototype Implementation of a Security Attribute Service in X.500'
M Jurečič, H Bunz, *Fairfax 94 pp 30–38*

The authors discuss the constraints on healthcare security policies in the context of German data protection law. The creator of a medical document has responsibility for it, but access rights can change in complex and dynamic ways. They describe an AIX/ISODE implementation which uses the X.500 directory structure for public key and privilege attribute certificates, and discuss the privilege management in detail.

041145 'The Electronic Motorist'
RK Jurgen, *IEEE Spectrum (Mar 95) pp 37–48*

The author provides an overview of in-car electronics including systems for security, safety and navigation, and possible interactions between these.

041146 'The Design and Implementation of Tripwire: A File System Integrity Checker'
GH Kim, EH Spafford, *Fairfax 94 pp 18–29*

The authors describe a tool developed to enable Unix system administrators to monitor changes to their file system. It uses message digest techniques to detect these, and can be configured to filter out most routine changes. They compare it with existing products — COPS, TAMU, Hobgoblin and ATP.

041147 'Challenge control on challenge-response type human interactions'
K Kobara, H Imai, *JW-ISC 95 pp 5–14*

This paper explains a general scheme of challenge-response human identification, and considers its security. It considers the mean number of trials needed for an attacker to spoof the system, and proposes a security evaluation method based on analysing the history of challenges.

041148 'Security requirements for Voice Messaging Operations'
G Kovacich, *Network Security (Feb 94) pp 15–18*

The author describes the security policy which should be adopted for a PBX with voice messaging, and the procedures needed to support this. There is a significant organisational problem, in that the PBX is usually seen to fall outside the security manager's domain.

041149 'A Taxonomy of Computer Program Security Flaws'
CE Landwehr, AR Bull, JP McDermott, WS Choi, *ACM Computing Surveys v 26 no 3 (Sep 94) pp 211–254*

This long survey article gives details of 50 computer security flaws which had previously been reported in the open literature. They occurred in a range of systems from MVS through Multics and Unix to PCs, and are classified by whether their introduction was accidental or deliberate, by the mechanism affected, by the flaw location, and by whether the introduction occurred during specification, coding, maintenance or operation.

041150 '50 years After breaking the Codes: Interviews with Two Bletchley Park Scientists'
JAN Lee, G Holtzmann, *IEEE Annals of the History of Computing v 17 no 1 (Spring 1995) pp 32–43*

This article provides some background information on British codebreaking in the second world war, and then presents an interview with two of its veterans — Jack Good and Donald Michie. This contains a lot of background material on personalities and organisation, as well as snippets such as that their main technical contribution to Colossus was a means (not discussed) of inferring the wheel patterns.

041151 'Doing it the Pick 'n Pay way'

R Martin, *Cards International (12/12/94) p 11*

South Africa's largest retailer has set up its own debit card system in order to collect transaction fees previously paid to the banks. They are concerned that a new smartcard scheme may enable the banks to regain control.

041152 'Concept of an electronic retail payment system with distributed control'

T Matsumoto, *JW-ISC 95 pp 24–33*

This article introduces an electronic retail payment system to provide flexible and efficient funds transfers, while maintaining security, reliability and anonymity. Funds are located on cards, and can be transferred to other cards via intelligent terminals, which periodically sent audit information to the banks.

041153 'On interactive human identification scheme'

T Matsumoto, R Mizutani, *JW-ISC 95 pp 1–4*

The authors report on a question-answer password identification scheme, and discuss its resistance against attack.

041154 'Attack of the hackers'

H McKenzie, *Banking Technology (Mar 95) p 20*

PBX and other telephone toll fraud is growing rapidly, especially in the USA and is estimated to cost phone companies $500m a year. It is now dominated by organised crime, and insurance can be bought to cover it .

041155 'Network if you can get it'

M Meredith, *Scottish Banker (Feb 95) pp 3–5*

This article provides a bankers' perspective of the opportunities and threats of the Internet. There is a shortage of commercial credibility, which banks can help to fix.

041156 'Multi-user quantum cryptography'

Y Mu, YL Zheng, Y Lin, *ISITA 94 pp 245–250*

The authors extend Bennett-Brassard's key distribution protocol to multi-user cryptography. Two basic configurations of communication channel, the so-called fan-shaped and series configurations, are considered; it is shown that many other configurations can be obtained from them, and that the systems are secure against intercept/resend attack.

041157 'Countering the counterfeiters'

J Newton, *Cards International (21/12/94) p 12*

Card fraud is endemic in China; counterfeiters felt safe from arrest until a joint China/Hong Kong initiative in May 94. Since then, counterfeit card factories have been raided in Beijing and Shantou; these had been using legitimate VISA and Mastercard holograms which the manufacturers had apparently been duped into supplying. However, there are probably over 100 hologram makers in China with the skills to produce passable forgeries.

041158 'Close to the nerve'

M Norton, *Banking Technology (Dec 94/Jan 95) pp 29–31*

Fraud cost VISA $655m worldwide last year, or 0.2% of turnover, at which rate it has been constant for some time. The organisation has run successful trials of neural network technology which tries to identify out-of-pattern transactions, and has also supplied 300 terminals to let US immigration officers check the validity of cards found on suspects.

041159 'Software glitch leads to crime by ATM gang'

M Norton, *Banking Technology (Mar 95) p 5*

Thieves in Oregon stole $364,770 by making 724 ATM withdrawals over 54 hours with a stolen card from a credit union whose ATM software was undergoing reconfiguration. Withdrawals should have been limited to $200 a day.

041160 'A design of scrambler using the flexible band pass filter'
SY Park, HS Lee, DK Lee, *JW-ISC 95 pp 94–100*

This paper describes an analog scrambler using variable band split frequency inversions.

041161 'Commercial off-the-shelf products — military panacea or financier's expedient?'
R Pengelley, *International Defence Review v 28 (Feb 95) pp 47–50*

This article describes a number of military applications running on commercial equipment, including Inmarsat B communications kit used by US special forces in Haiti and the lap top PCs in general use by the US army. Commercial systems tend not to support NATO messaging standards, or Ada; and their upgrade cycles, warranty conditions and IPR arrangements are not generally to soldiers' liking. The UK solution is the 'Security in Open Systems' project, which aims to develop a security architecture acceptable for both government and civilian users.

041162 'Caught in a fragile net'
P Penrose, *Banking Technology (Feb 95) pp 26–28*

This article discusses some of the weaknesses of the ECU clearing system, which is considered one of the most fragile banking systems in Europe; it needs legal clarification, stronger risk management and a lender of last resort.

041163 'The next generation'
P Penrose, *Banking Technology ((Mar 95) pp 22–26*

This article discusses Internet banking, including First Virtual Holdings, DigiCash, and the joint venture between Microsoft and VISA. VISA describes its partner as being 'after (the banks') dinner' but justifies the partnership in terms of the banks' need to continue to do business.

041164 'Army links to cashcard'
FB Ping, *Smart Card Bulletin (Dec 94) p 1*

The Singapore Ministry of Defence is introducing a card for all military personnel, which will not only be an ID but also control computer access, encrypt data, track stores, book facilities, act as an electronic purse, and manage incentives for performance in fitness tests and range practices.

041165 'Post Office to automate with cards'
C Power, *Cards International (21/12/94) p 3*

The UK Post Office will next year award a £200m contract to move welfare payments from paper books to smartcards; five shortlisted suppliers have been announced.

041166 'Interworking between Digital European Cordless Telecommunications and a distributed packet switch'
S Rao, DJ Goodman, GP Pollini, KS Meier-Hellstern, *Wireless Networks v 1 (Feb 95) pp 83–93*

The authors discuss hoe to connect a DECT network to a distributed system, and discuss some of the authentication aspects of call setup and location update.

041167 'Network Security Probe'
P Rolin, L Toutain, S Gombault, *Fairfax 94 pp 229–240*

The authors describe a tool called NSP which detects network intrusion, and also provides authentication and audit facilities for selected applications.

041168 'The Colossus of Bletchley Park'

AJ Sale, *IEE Review, March 1995 pp 55–59*

The author describes a project to reconstruct the Colossus, an early computer used at Bletchley Park for correlation attacks on the Lorentz Geheimschreiber. This used hundreds of thyratrons to simulate the rotor wheels and counters to keep track of pattern matches. This machine would process intercepts at 5000 characters per second — the speed at which the paper tape could be fed — and could break a key setting in 2-3 days. Although its secrecy meant that it had no direct impact on subsequent computing history, it had an indirect effect in that it showed Turing and others that digital machines with thousands of valves could be made to work reliably.

041169 'Coding for Distributed Computation'

LJ Schulman, *Info Theory 94 p 28*

The author discusses the impact effect of noisy links in a computer network when it comes to performing a distributed computation. This paper may be consider when looking at the hook up problem in secure networks.

041170 'MultiSix: How it Improves Interoperability in a Multi-Vendor Network'

S Scudamore, *ACM SIGSAC v 13 no 1 (Jan 95) pp 12–16*

This paper describes DEC's trusted network architecture which supports DNSIX, CMW, trusted X, Trusted TCP/IP and Trusted NFS.

041171 'Netscape opens Internet to cards'

S Smith, *Cards International (11/1/95) p 6*

Netscape's new secure browser, together with its commerce server, can now process credit card transactions through six acquiring banks.

041172 'Internet: Zielscheibe für Hacker'

D Sticharz, *Datenschutzberater v 19 no 2 (15/2/95) pp p–4*

The author describes some recent security incidents on the Internet, including an assault on the San Diego Supercomputer Center in December which used IP address spoofing. Attacks on routers are also described and references are given to a number of CERT advisories.

041173 'Bolero trade steps'

S Talmor, *The Banker (Feb 95) pp 72–75*

The EC's Bolero project, to develop and pilot an EDI system for bills of lading, is due to finish in July. As these bills carry value as well as information, they are digitally signed, with secret keys managed using smartcards; there is also a central registry, whose main purpose is to stop banks obtaining all the trading information of payees. Perceived benefits to traders include cutting errors and processing costs, while banks are concerned to integrate bills of lading with letter of credit systems.

041174 'Faster, ever faster'

I Tredinnick, *International Security Review no 87 (Winter 94/5) pp 17–18*

ISDN lines may find an important application in video surveillance; they increase the frame rate from 1 per 3 seconds to 4–6 per second.

041175 'A signature scheme using a compiler'

K Usuda, M Mambo, T Uyematsu, E Okamoto, *JW-ISC 95 pp 111–119*

The authors describe a signature scheme for virus protection: it reassures the programmer that his executable programs are signed without being infected with a virus.

041176 'Is anyone listening?'
N van der Bijl, *International Security Review no 87 (Winter 94/5) pp 20–22*

This article discusses the industrial espionage business, and discusses both equipment sales and the legal/technical countermeasures. It concludes however that the main threat remains the subversion of trusted employees, and relates the story of the Europark operation against NCP which led to criminal prosecutions in the UK.

041177 'Image scrambling for DCT-based image compressions'
CS Won, JI Kwon, JK Kim, *JW-ISC 95 pp 101–110*

This paper proposes a two-step image scrambling method: first the DCT-block gray-level is scrambled, then the DCT coefficients are too.

041178 'Fighting mobile phone fraud'
K Wong, *Computer Fraud and Security Bulletin, Jan 95 pp 9–16 (part 1), Feb 95 pp 10–14 (part 2)*

In Britain alone, 15,000 mobile phones are stolen each month, and unauthorised reprogramming of analogue phones adds a considerable further loss. Fraud against digital phones currently involves service applications in false names, but it is expected that subscriber identity modules will be broken within a year or two. Most antifraud measures are common sense, although some technical fixes are emerging; a structural problem is that security takes second place to marketing.

041179 'Application of Hidden Markov Models for Signature Verification'
L Yang, BK Widjaja, R Prasad, *Pattern Recognition v 28 no 2 pp 161–170*

The authors describe using a Hidden Markov Model to verify signatures. These are digitised with a graphics tablet and modelled with successions of pen-down and pen-up symbols; the latter compensate for accumulated distortion. The more symbols, the more distortion can be accommodated, but the longer the system takes to train. False acceptance rates of 5–15% and false rejection rates of 1–2.5% were obtained depending on the method used.

041180 'Security versus Performance Requirements in Data Communications Systems'
V Zorkadis, *ESORICS 94 pp 19–30*

The author applies queueing theory to analyse the effect which security mechanisms have on communications performance, and in particular the benefits of using an additive stream cipher with precomputation and how they depend on the load on the system.

2 Operating System and Database Security

041201 'The Evolution of MaxSix Trusted Networking'
JR Adams, DF Luther, *ACM SIGSAC v 13 no 1 (Jan 95) pp 7–11*

The authors describe TSIG, an industry initiative to develop interoperable trusted systems, which has led to an implementation called MaxSix. This extends DNSIX to provide session management with full security attributes.

041202 'An Efficient Multiversion Algorithm for Secure Servicing of Transaction Reads'
P Ammann, S Jajodia, *Fairfax 94 pp 118–125*

All current designs for replicated architecture MLS databases perform badly when loaded with long read-only transactions, as these can starve high level processes by blocking updates. The authors produce a new concurrency control algorithm which tackles this problem by maintaining versions of modified data. In return for having some processes see a slightly dated version of the database, the algorithm uses bounded storage and keeps concurrency control out of the TCB.

041203 'Compile-time detection of information flow in sequential programs'
JP Banâtre, C Bryce, D Le Métayer, *ESORICS 94 pp 55–73*

The authors propose a simple guarded command language for the formalisation of information flow in programs, which is designed to be easy to implement in a proof checking tool. They claim that it could be used to synthesise the weakest constraints on the security labels of variables in unannotated programs.

041204 'A Temporal Authorisation Model'
E Bertino, C Bettini, P Samarati, *Fairfax 94 pp 126–135*

The authors present a formal model of a discretionary access system for databases in which authorisations persist for only a finite period of time. They introduce a formalism to deal with temporal and other dependencies, and discuss the relationships between the various possible rules.

041205 'An Entropy Conservation Law for Testing the Completeness of Covert Channel Analysys'
R Browne, *Fairfax 94 pp 270–281*

The author defines a complete set of covert channels as one which can operate to produce the maximum covert information flow. He shows that such sets are characterised by their satisfying an entropy conservation law, in that a fully informed onlooker perceives an output uncertainty equal to the covert capacity plus the relevant noise. This in turn lets the system behaviour be expressed in a kind of normal form.

041206 'Distributed file system over a multilevel secure architecture — problems and solutions'
C Calas, *ESORICS 94 pp 281–297*

The authors describe the further development of the multilevel system M^2S (previously described in **021113**). This now possesses a multilevel distributed NFS-lookalike file system; only one of the machines need be multilevel, and most of the work can be done by system high file servers.

041207 'Access control with binary keys'
CC Chang, JJ Shen, TC Wu, *Computers and Security v 13 no 8 (94) pp 681–686*

The authors propose a kind of capability based access control system.

041208 'An Introduction to MVS Integrity Concerns'
N Crocker, *Network Security (Dec 94) pp 12–16*

IBM's MVS integrity statement sets the goal that no unauthorised program should be able to circumvent store or fetch protection, access RACF or password controlled resources, or obtain control in authorised state. However, this depends on many measures under user control, and the manual describing these has not been updated for ten years. Eleven of the potential problems are mentioned and three described in some detail — the IPL parameter library, supervisor calls and APF libraries.

041209 'Privilege Graph: an Extension to the Typed Access Matrix Model'
M Dacier, Y Deswarte, *ESORICS 94 pp 319–334*

The authors extend Sandhu's typed access matrix model to cope more efficiently with situations where a user can grant a large number of access rights at once. This works by introducing ad-hoc privileges which allow users of a given class to take up a given access right, and then chaining these together into a graph. real world examples involving .rhosts files and setuid privileges are given.

041210 'Implementing Secure Dependencies over a Network by Designing a Distributed Security SubSystem'
B d'Ausbourg, *ESORICS 94 pp 249–266*

The author describes the design of a multilevel secure LAN, which uses special interface hardware to allocate distinct time slots to traffic at different levels. Information flow analysis was carried out using a causality model, which attempts to track the cone of events which are affected by some given event.

041211 'The Operating System Kernel as a Secure Programmable Machine'
DR Engler, MF Kaashoek, JW O'Toole, *Operating Systems Review v 29 no 1 (Jan 95) pp 78–82*

The authors are developing an exokernel — a minimal operating system whose interface is at an even lower level than usual. The idea is to provide safe but almost direct access to the hardware by controlling resource allocation, deallocation and multiplexing. In order to reduce the load on the TCB, user code can be run in supervisor mode provided it satisfies a number of safety criteria. The idea is to allow security policies to be tailored to the hardware and run with very little overhead.

041212 'Worldwide Smart Card Services'
A Gamache, P Paradinas, JJ Vandewalle, *Cardis 94 pp 141–148*

The authors propose a new agent-based paradigm for smartcard security; that encapsulated applications be stored outside the card, and data on it. This way, the card would become a secured execution environment for suitably authorised programs. It is argued that this structure will provide the best environment for multiple service providers to access common data.

041213 'Authentication via Multi-service Tickets in the Kuperee Server'
T Hardjono, J Seberry, *ESORICS 94 pp 143–160*

The authors describe the cryptographic protocols used in Kuperee, a prototype distributed operating system. These use public key techniques to facilitate dual control, parallelism and multiple domains, and to limit the damage which can be caused by the compromise of a security server.

041214 'Database authentication revisited'
T Hardjono, YL Zheng, J Seberry, *Computers and Security v 13 no 7 (94) pp 573–580*

The authors discuss using their idea of sibling intractable function families to provide crypto checksums for databases. The idea is that a single checksum on each record can authenticate each data element separately.

041215 'Towards testability in smart card operating systems design'
PH Hartel, EK de Jong, *Cardis 94 pp 73–88*

The authors discuss how smartcard operating systems can be designed with a reasonable degree of assurance. The goal is to achieve an ITSEC rating of E5 or better, and the chosen route is a secure instruction set interpreter based on functional programming ideas; this will parse terminal traffic and call application code routines. The proposed system has been prototyped.

041216 'Robust and Secure Password and Key Change Method'
R Hauser, P Janson, R Molva, G Tsudik, E van Herreweghen, *ESORICS 94 pp 107–122*

The authors describe the password change mechanisms of KryptoKnight. They discus the design requirements and compare it with the kerberos mechanism, which they show to be vulnerable to guessing attacks. Their basic idea is to make the change work whether the authentication server knows the old password or the new one; this makes it more robust in the face of replay attacks.

041217 'The Compatibility of Policies'
HM Hinton, ES Lee, *Fairfax 94 pp 258–269*

The authors call two security policies compatible at a given system if it satisfies them both simultaneously. Policies can be incompatible for environmental as well as technical reasons, and a model is developed with reference to railway signalling. This model is then applied to discuss confidentiality, integrity and faithfulness (that the same inputs will give the same outputs); these are shown to be compatible.

041218 'A design and implementation of secure system calls for enforcing security model'
KY Hong, DK Kim, *JW-ISC 95 pp 228–237*

In this paper, a design of security mechanisms is presented to enforce a security model from the viewpoints of preserving discretionary access control, mandatory access control, and label policies.

041219 'Support for the File System Security Requirements of Computational E-Mail Systems'
T Jaeger, A Prakash, *Fairfax 94 pp 1–9*

Many collaborative applications can be built using email scripts which execute upon receipt, yet this brings obvious perils. The authors briefly describe the features and problems of Atomicmail, Safe-Tcl, Telescript and Mosaic, and propose a security model which allows execution of email from trusted senders without compromising private files. The key idea is careful treatment of the intersection between the private and public filespace. Finally, they discuss how to implement it using AFS, Unix or the Safe-Tcl interpreter.

041220 'A message server access control model enforcing multi security policies'
SW Kim, DK Kim, *JW-ISC 95 pp 201–208*

The authors model a secure message server in an environment with multiple security policies.

041221 'An active object-oriented database model with multilevel security constraints'
Y Kim, C Lee, B Noh, *JW-ISC 95 pp 209–218*

This paper proposes an active object-oriented model which represents active rules in a conceptual schema by event and rule objects. This model can be used as a database design tool, and security requirements of active rules on applications can be easily captured using this model.

041222 'Coding for Noisy Feasible Channels'
RJ Lipton, *Info Theory 94 p 27*

The author discusses the idea of a feasible channel. This is a channel where encoding/decoding is all in polynomial time, along with some other more minor criteria. These channels might be a realistic class to consider for covert channel analysis.

041223 'Design for dynamic user-role-based security'
I Mohammed, DM Dilts, *Computers and Security v 13 no 8 (94) pp 661–671*

The authors describe a role-based security model developed for a medical application in Canada which combines features of mandatory and discretionary access control. For example, the computer record of a letter may not be changed once a physical copy of it has sent. Design and implementation details are also discussed.

041224 'Discussion of a Statistical Channel'
IS Moskowitz, MH Kang, *Info Theory 94 p 95*

This paper discusses a new type of timing channel called a statistical channel. A discussion is given of how statistical techniques may be used to analyze subtle variations in response time. Applications to the NRL Pump are discussed.

041225 'Security Through Type Analysis'
C O'Halloran, CT Sennett, *ESORICS 94 pp 75–89*

The authors discuss a project to automatically analyse compiler output in TDF format to and ensure that software modules cannot be called with arguments which they should not handle. The principal mechanism is type inference, and the main problem is coping with pointer arithmetic. A case study is presented of a multilevel secure file transfer mechanism, and the type checking algorithm is described.

041226 'A simple way to control information flows'
S Ozaki, T Matsumoto, H Imai, *JW-ISC 95 pp 43–52*

The discretionary access control method adopted by UNIX is simple and understandable, however unexpected information flows can occur when group members cooperate. Introducing notions such as maximal permission and multiple groups associated to a single file, this paper proposes a method to control these indirect information flows.

041227 'New Directions for Integrated Circuit Card Operating Systems'
P Paradinas, JJ Vandewalle, *Operating Systems Review v 29 no 1 (Jan 95) pp 56–61*

The authors discuss the requirements for the next generation of smartcard operating systems. These will need to be much more modular and flexible than current offerings, and an object-oriented approach is suggested.

041228 'Dangerous Letters: ANSI Bombs and Forged E-mail'
P Peterson, *Network Security (Dec 94) pp 17–19*

The author reports creating a PC virus all of whose op codes were printable ASCII characters — in fact it was a Christmas card. Methods of forging email and remapping the keyboard can also give rise to unconventional and unexpected attacks.

041229 'Extended labeling policies for enhanced application support'
J Picciotto, RD Graubart, *Computers and Security v 13 no 7 (94) pp 587–599*

The authors describe an operating system level mechanism for enforcing labeling on portions of files rather than on whole files. This fine granularity can be useful in many applications, such as in a multilevel secure spell checker; it was prototyped in a Unix CMW mail system and editor. Blind write-up is not supported, as clashes could not be detected even in principle; implementation options are discussed.

041230 'A Security Language For The Card: The S-Shell'
JM Place, P Trane, *Cardis 94 pp 33–48*

The authors discuss the requirements for an implementation independent security language which would cope with a variety of operating systems, databases and microprocessor cards. The shortcomings of Unix and MCOS are described, as is a prototype shell which is essentially a state machine acting on a description file, together with naming conventions for secret data.

041231 'An Authorization Model for Personal Databases'
C Radu, M Vandenwauver, R Govaerts, J Vandewalle, *Cardis 94 pp 61–72*

The authors describe a database security model for smartcards which came out of their work with CAFE. This is centrally administered, role and capability based, and has a granularity hierarchy of objects with a tree structure; each capability gives access to everything below the node it names.

041232 'A Security Architecture for Fault-Tolerant Systems'
MK Reiter, KP Birman, R van Renesse, *ACM Transactions on Computer Systems v 12 no 4 (Nov 94) pp 340–371*

The authors describe Horus, an architecture for distributed systems based on secure process groups. Its underlying mechanisms are founded on fault tolerant authentication protocols, some of which are described, and a secure time service. These mechanisms are implemented in a layer which is inaccessible to user processes.

041233 'Non-interference through Determinism'
AW Roscoe, JCP Woodcock, L Wulf, *ESORICS 94 pp 33–53*

The authors consider noninterference in terms of the nondeterminism introduced into an abstract machine by hiding and interleaving operations, and propose to protect low users from high data by insisting that their virtual machines be deterministic. Under this definition, security is preserved by refinement. A file system design is sketched, and the relationship between Z and CSP formalisms is discussed.

041234 'Propagation of Authorizations in Distributed Database Systems'
P Samarati, P Ammann, S Jajodia, *Fairfax 94 pp 136–147*

Authorisations which propagate in distributed systems may do so inconsistently, especially in the presence of intermittent site and communications failures. Algorithms are presented for restoring consistency; logs of authorisation table updates are kept locally and propagated, and procedures exist for dealing with out-of-order updates by referring to these logs.

041235 'On the Expressive Power of the Unary Transformation Model'
RS Sandhu, S Ganta, *ESORICS 94 pp 301–318*

The authors develop their transformation model of access control by introducing a variant in which individual commands can test only one cell of the access control matrix at a time. They prove that this has just as much expressive power, provided that every user and every object can be constrained to be of a unique type.

041236 'To Net Or Not To Net?'
W Schwartau, *Network Security (Dec 94) pp 7–11*

The author describes a product called Sidewinder, whose purpose is to enforce a multilevel integrity policy in an Internet environment.

041237 'Total ordered security level assignment which inhibits entity inference'
H Shina, Y Okuda, H Nagase, *ISITA 94 pp 273–276*

The authors propose an algorithm to assign security labels to entities in a computer system in accordance with a model such as Bell-LaPadula. The proposed algorithm generates the highest security label for each entity. This is in contrast to the low water mark principle which assigns the lowest label to each entity.

041238 'CMW Information Labels: A DBMS Perspective'
D Sidwell, T Ehrsam, *ACM SIGSAC v 13 no 1 (Jan 95) pp 2–6*

The lack of standards for information labels in MLS and especially CMW systems is a serious headache for application software vendors. Some label management strategies used by various DBMS suppliers are discussed.

041239 'A Secure Medium Access Control Protocol: Security versus Performances'
P Siron, B d'Ausbourg, *ESORICS 94 pp 267–279*

The authors report how they measured the performance cost of adding multilevel security to a LAN (as described in d'Ausbourg above). The main tool was simulation using NETSIM, and the exercise concluded that for a small number of security levels the performance degradation was negligible.

041240 'Modeling and verification of indirect information flow based on hierarchical time petri net'
M Tetsuya, T Shigeo, *JW-ISC 95 pp 53–60*

This paper describes modeling and verification of indirect information flow using a Hierarchical Time Petri Net (H-TPN), on which both information and users are described by places.

041241 'Networked Multimedia: the Medusa Environment'
S Wray, T Glauert, A Hopper, *IEEE Multimedia (Winter 94) pp 54–63*

The authors describe a second generation peer-to-peer multimedia architecture developed at Olivetti. It is based on ATM, and access control uses one-time capabilities which are exercised through proxies, which give temporary access but can be revoked easily. Proxies filter transaction requests to the modules they protect, and can also monitor changes in attributes. In effect they are firewalls which isolate the trusted modules from the rest of the system. For example, all software modules are created in factories, which in turn are controlled by proxies. Another feature is that connections are reliable, in the sense that either the data will arrive safely or the connection will be irrevocably destroyed.

3 Security Management and Policy

041301 'IT security in the financial sector'
C Amey, *Computer Fraud and Security Bulletin (Jan 95) pp 16–19*

As banking systems get more complex, they become less secure, and the only real response is managerial — through risk assessment, documentation, education and design stage application review. The role of technical measures such as authentication servers is that they can help to recentralise some of the control.

041302 'A Process-Oriented Methodology for Assessing and Improving Software Trustworthiness'
E Amoroso, C Taylor, J Watson, J Weiss, *Fairfax 94 pp 39–50*

Various US military agencies and contractors and contractors have been working since 1989 on a methodology for assessing the amount of trust which can be placed in a piece of software. The result is a set of trust classes ranging from T0 (no trust) to T5 (the highest level). As with the Orange Book, there is a matrix of increasing trust requirements, which is given; and the authors also describe the rationale behind the design. This combines elements of ISO 9000, CMU SEI's capability maturity model, and existing defence methodologies, and is heavily oriented to the software process rather than to the final product.

041303 'Security Modelling for Organisations'
A Anderson, D Longley, FK Lam, *Fairfax 94 pp 241–250*

The authors discuss how security officers can use models of the systems under their protection to communicate with managers, to estimate the effectiveness of threat models, and to assign value to intangible assets such as confidence.

041304 'Liability and Computer Security: Nine Principles'
RJ Anderson, *ESORICS 94 pp 231–245*

The author discusses recent experience in the UK and elsewhere of legal disputes involving cryptographic evidence. One of the most powerful tactics in such cases is to challenge security claims by pushing for disclosure of the other side's security mechanisms; this has been granted by a number of courts, leading to the collapse of prosecution cases. Computer security mechanisms whose purpose is to provide evidence must therefore be designed to withstand scrutiny from hostile experts. Further problems are caused by the fact that many security systems are really intended to shift blame rather than to stop attacks, and this fact itself is concealed; and from system designers' lack of understanding of how the legal system actually works.

041305 'Daten- und Informationssicherung (IS) als strategische Gesamtlösung'
R Apitzsch, *Datenschutzberater v 19 no 2 (15/2/95) pp 6–10 (in German)*

The author discusses the security consulting approach of IBM Deutschland. This focusses on building complete solutions to all an organisation's security and disaster recovery requirements.

041306 'Secure the Virtual Office'
DS Bernstein, *Datamation (15/1/95) pp 49–52*

The author discusses basic computer security and gives a list of vendor contacts.

041307 'The Clipper Chip and the Price of Security in America'
JR Butler, KA Forcht, *Information Management and Computer Security v 2 no 5 (1994) pp 9–12*

The authors talk about the Clipper chip; they describe in general terms how it works and discuss some of the political issues raised.

041308 'Database detection methods in criminal investigations'
V Collins, *Computer Law and Security Report v 15 no 1 (Jan/Feb 95) pp 2–11*

The author describes a number of recent developments in computer law which have civil liberties implications, such as the conviction of a rapist from a DNA record which ought to have been destroyed. As the amount of retained information increases, both data protection and the restraints on evidence admissibility tend to be eroded. The potential for abuse exists in many areas, including email messages and the profiling of purchase patterns, and increasing international police cooperation (such as that forced by the Schengen agreement) will broaden the scope for abuse.

041309 'Disaster recovery: before it's too late'
Computer Fraud and Security Bulletin (Mar 95) pp 10–14

The author provides yet another potted guide to contingency planning.

041310 'Testing the Disaster recovery Plan'
J Cooper, B Edwards, *Computer Audit Update (Dec 94) pp 3–11*

Contingency plans can be tested at a number of levels, from a full live test through module and component tests through procedural dry runs. In each case, the best value is only obtained with explicit goals and thorough planning.

041311 ' "Mainstreaming" Automated Information Systems Security Engineering (A Case Study in Security Run Amok)'
JW Coyne, NC Kluksdahl, *Fairfax 94 pp 251–257*

The authors discuss a series of events at NASA's mission control center in Houston. After the end of military missions at this facility, a security team was set up to fill the vacuum left by the end of DoD compliance. This team was given an ambitious charter, and became independent of both the development and operations teams. Its impositions became increasingly unrelated to budget and operational constraints, and its relations with the rest of the organisation became increasingly adversarial. In the end, security was taken over by the team responsible for budgets and moved from a compliance-based to a risk-based approach, which is described in some detail.

041312 'Insuring computer related risks — a challenge for the 90's'
D Davies, *Computer Law and Security Report v 14 no 6 (Nov/Dec 94) pp 313–316*

The author discusses what can go wrong when buying computer insurance and provides a number of illustrative anecdotes. The main problem is that the computer and insurance people do not talk the same language; indeed, there are even computer insurance proposal forms which betray profound ignorance.

041313 'Tricks of the LAN security trade'
F Doyle, *Network Security (Nov 94) pp 12–13*

The author discusses security policies and plans which are appropriate for LANs.

041314 'Internet ethics'
B Duran, *Computer Fraud and Security Bulletin (Feb 95) pp 14–16*

The author discusses the evolution of ethics among both hackers and the general Internet community.

041315 'Ultra and Some US Navy Carrier Operations'
R Erskine, *Cryptologia v XIX no 1 (Jan 95) pp 81–89*

The author describes the measures taken by the Allies to protect the security of Ultraintelligence in the battle of the Atlantic. This was not too difficult so long as it was only used to route convoys around U-boat packs, but much trickier when it was later used to target and sink U-tankers.

041316 'Fraud prevention and computer security for financial institutions'
J Essinger, *Computer Fraud and Security Bulletin, Feb 95 pp 17–19 (part 1) and Mar 95 pp 16–19 (part 2)*

The author gives a broad overview of the types of control that are, or could be, implemented in a banking computer environment.

041317 'The Information Highway'
KA Forcht, M Oare, *Information Management and Computer Security v 2 no 5 (1994) pp 4–8*

The authors discuss some of the business and legislative background to the 'Information Highway', including problems with charging, copyright, access control and other security concerns.

041318 'Herstellung vertrauenswürdiger IT und Praxis der IT-Sicherheit'
D Fox, *Datenschutzberater v 19 no 3 (15/3/95) pp 10–12*

This article reports two seminars held by the German information security agency in January on security engineering. They covered quality, reliability and certification aspects of the subject. Some 25 products are put forward for certification each year in Germany.

041319 'Security Evaluation in Information Technology Standards'
F Gentile, L Giuri, F Guida, E Montolivo, M Volpe, *Computers and Security v 13 no 8 (94) pp 647–650*

The authors discuss hidden dependencies in evaluation, such as when a standard based on a poor product is then used as a basis for an evaluated product. They suggest that a process for evaluating standards is required.

041320 'Disaster Planning Comes to Frame Relay'
R Goreiss, *Data Communications International (Mar 95) pp 51–52*

A US telecomms service provider has come up with the idea of offering a full backup network for only half the price again of a client's primary network.

041321 'Assessing and Reducing Network Risk'
W Hancock, *Network Security (Feb 95) pp 7–8*

The network is now many companies' most critical asset, and communicating this to users is the first step in building a realistic threat model. Contingency plans must include a troubleshooting methodology; an example is given where a US company was almost closed down by an unexpected loop which caused flooding, but the users were reluctant to believe that the fix involved killing a new router.

041322 'Promoting computer security through positive computer audit'
G Hardy, *Computer Audit Update (Jan 95) pp 12–19*

Making the audit checklists public can gain the support of other staff and thus make the exercise more positive and effective. The DTI/BSI code of practice may provide a foundation for this; its audit aspects are discussed.

041323 'Elektronische Autobahnmaut'
G Hohlweg, *Datenschutzberater v 18 no 12 (15/12/94) pp 4–7 (in German)*

This article discusses the data protection aspects of automated motorway tolling in Germany. Some of the proposed systems are strongly criticised, and it is argued that a smartcard-based electronic cash system should at least be an option. The video surveillance systems used to catch non-payers and to monitor traffic also pose a privacy problem.

041324 'Opportunity Makes a Thief — A Report on Computer Abuse from the Audit Commission'
C Hurford, *Computer Audit Update (Dec 94) pp 12–15*

The UK government recently surveyed computer abuse in both private and public sectors; the responses were dominated by local government, health care and manufacturing. Compared with the last survey in 1990, there was a large increase in viruses, illicit software and unauthorised private work. The unauthorised disclosure of private information was reported for the first time, mostly in the state sector.

041325 'British government mulls ID card technology'
Information Security Monitor v 10 no 3 (Feb 95) p 1

The UK government has been forced by leaks to admit that it is considering a national identity card scheme, which may be announced in the spring. The last ID cards were scrapped in 1952.

041326 'Managing the security of new technologies in a diverse business environment'
Information Security Monitor v 10 no 2 (Jan 95) pp 5–7

This article describes the security management approach taken by National Power, the UK's largest electricity generator.

041327 'Enterprise Security'
JJ Johnson, *Data Communications International (Mar 95) pp 110–127*

The author provides a survey of available authentication, encryption and authorisation products, listing seventeen US suppliers. He explains the workings of products such as password generators and Kerberos.

041328 'EU-Datenschutzrichtlinie: Gemeinsamer Standpunkt beschlossen'
F Kopp, *Datenschutzberater v 19 no 3 (15/3/95) pp 1–7 (in German)*

The new European data protection guidelines were adopted in February after four years of negotiation. These became a battle between the French model of state control and the German one of self control with state oversight (which won out). The goal is to provide a coherent data protection policy for Europe which can tackle new problems such as interactive TV (which allows psychological profiling of the viewer) and mobile communications (which betray his location). Member states must legislate along these guidelines by 1999.

041329 'Local Area Network Security: Establishing Policies and Procedures'
GL Kovacich, *Network Security (Jan 95) pp 13–16*

This article presents a suggested LAN security policy and describes the documentation and procedures needed to support it.

041330 'The Cyberpunk Age'
K Lindup, *Computers and Security v 13 no 8 (94) pp 637–645*

The author presents some nuggets gleaned from SRI interviews with many hackers and ex-hackers in the USA and Europe. He mentions a number of clubs and groups, and discusses the social engineering techniques often used to obtain sensitive information over the telephone.

041331 'Online Industrial Espionage'
W Madsen, *Network Security (Nov 94) pp 14–18*

The end of the cold war has left national intelligence agencies searching for new missions, and many have turned to industrial and economic espionage. A number of incidents are recounted, and the structure of commercial intelligence gathering in France and Germany are discussed.

041332 'The Clipper Controversy'
W Madsen, *Network Security (Nov 94) pp 6–11*

The author describes the evolution of US crypto policy from the foundation of the NSA to the Clipper chip and its cognate programs such as DSS, CATAPULT, Operation Root Canal and secure Mosaic.

041333 'US government board to create "New Security Order" '
W Madsen, *Computer Fraud and Security Bulletin (Feb 95) pp 8–9*

The author discusses the US Security Policy Board, which was established by President Clinton to harmonise the classified and nonclassified approaches to information protection, and to lay down policy on the effects of sexual orientation on clearance, surveillance countermeasures, Tempest, and the training of security personnel. He claims that it will subordinate NIST to the NSA for this purpose.

041334 'Who's Guarding the Till and the CyberMall?'
L Marion, *Datamation (15/2/95) pp 38–41*

The author discusses the security concerns of electronic commerce, and contrasts the EDI and Internet approaches.

041335 'Understanding Backups — A Business Perspective'
J Maynard, *Computer Audit Update (Dec 94) pp 15-18*

The business goals of backup often get obscured by the technology; many firms spend most of their effort backing up multiple copies of applications code rather than actual business data.

041336 'Secure Unix for Enterprise Computing'
RJ Melford, *Datamation (1/3/95) pp 55–58*

The author discusses the basics of Unix security.

041337 'The economics of network security'
D Moreley, *International Security Review (Winter 94/5) pp 23–26*

The author, a general manager at Cylink, describes a number of computer security products from his own and other companies.

041338 'Development of Security Policies'
J Ølnes, *Computers and Security v 13 no 8 (94) pp 628–636*

The author discusses how to go about developing an organisational security policy.

041339 'The court's perspective on defective computer systems: lessons to learn'
R Parry, *Computer Audit Update (Feb 95) pp 3–6*

In a recent case (The Salvage Association v CAP Financial Services Ltd), the court set aside a clause limiting damages to £25K on the grounds that the defendant had insurance for £500K while the plaintiff had no means to insure against the risk.

041340 'The Enigma of Bletchley Park — World War II Codebreaking to Museums Campus'
AJ Sale, *Cirencester 93 pp 73–81*

The author gives a brief history of British codebreaking at Bletchley Park during the second world war, and describes current moves to set up museums of cryptology, computing, radar and electronics on the site.

041341 'Electronic Monitoring Poses Email Dilemma'
S Saxby, *Network Security (Jan 95) pp 17–18*

The Privacy Commissioner of Ontario has recommended that firms respect users' email privacy, and in the USA, Federal guidelines on employee monitoring have been proposed (but failed to get through Congress). The EU's data protection directive will have similar effects. Thus monitoring will increasingly require notice and/or consent.

041342 'How Hackers Do It'
R Schifreen, *Network Security (Oct 94) pp 17–19*

The author presents a list of thirty nine techniques which hackers have used (or could use) to defeat network security.

041343 'Password alternatives'

W Schwartau, *Network Security, Jan 95 pp 9–13 (part 1); Feb 95 pp 13–15 (part 2)*

The author discusses passwords and their alternatives, such as passphrases, smart diskettes, other tokens and biometrics.

041344 'Industrial Espionage: Analysing the Risk'

P Sommer, *Computers and Security v 13 no 7 (94) pp558-563*

The author discusses the context of industrial espionage. Ninety percent of the useful information about a company is already in the public domain, and can be gathered at no risk. Whether the other ten percent will be targeted is a function of the client's business ethics more than anything else. Methods of developing a threat model for a client which wishes to defend itself are discussed.

041345 'The BSA software crimeline'

R Taylor, *Computer Audit Update (Mar 95) pp 11-14*

An association of UK software vendors is offering a reward to people who inform on the users of unlicensed software.

041346 'The management of computer security profiles using a role-oriented approach'

SH von Solms, I van der Merwe, *Computers and Security v 13 no 8 (94) pp 673–680*

The authors discuss how a security manager can go about constructing models of user roles in a systematic manner. It is especially desirable that exception reporting should be nontechnical and comprehensible to personnel management.

041347 'The Internet Threat'

H Wolfe, *Network Security (Jan 95) pp 7–8*

The author surveys hackers' magazines and other information sources, and describes some of the toolkits available for virus writing and password cracking.

041348 'New developments in information technology to combat computer crime and fraud'

K Wong, *Information Security Monitor v 10 no 4 (Mar 95) pp 5–8*

The author describes the new British Standards Institute security code of practice which makes recommendations for organisations' policy, plans and controls. He also talks about a number of security products.

041349 'Identity token usage at American commercial banks'

CC Wood, *Computer Fraud and Security Bulletin (Mar 95) pp 14–16*

A survey of 35 banks showed that 89% of them used some kind of 'extended user authentication', i.e. did not rely on password based access control alone. The majority used password generators, and the next most popular technique was transparent challenge-response; these techniques were typically implemented at a front end processor or firewall. Case law indicates that, at least in the USA, a security control becomes part of the standard of due care once 33–40% of the firms in an industry use it.

041350 'The use of the PC as a network audit tool'

P Wood, *Computer Audit Update (Mar 95) pp 5–10*

According to the author, Netware suffers from a serious lack of internal security management tools, which leads to many users being given supervisor status for reasons of convenience. Yet there are no audit trails of supervisory status changes, directory creations and the like, and the system is so complex that manual tracking is unfeasible. This leads him to set forth a set of requirements for an automated security management tool.

041351 'The Verdict on Plaintext Signatures: They're Legal'

B Wright, *Computer Law and Security Report v 14 no 6 (Nov/Dec 94) pp 311-312*

It is often said that digital signatures are essential to make electronic commerce legally binding. This is untrue; the defining attribute of a signature is the signer's intent, and a plaintext name at the bottom of an email message has legal force. It may be easy to forge, but then so are the manuscript signatures which have been used for centuries *(see book review, this issue).*

041352 'Protecting information from Internet threats'

MA Wright, *Computer Fraud and Security Bulletin (Mar 95) pp 6–10*

The author describes some of the security problems of the Internet and possible countermeasures such as password discipline, firewalls and encryption.

041353 'EU-Datenschutzrichtlinie: Einigung im Rat'

Ulrich Würmeling, *Datenschutzberater v 19 no 2 (15/2/95) pp 4–5 (in German)*

A majority of the EU's Council of Ministers has ratified the European data protection guidelines. These cover structured manual data as well as computer files; the national jurisdiction to apply will be that of the data owner's head office, so that for example a German firm in France will fall under German law; purely automatic decisions are forbidden on matters important to an individual such as credit decisions; data subjects can demand directly from data owners information which does not have to be reported to the data protection authorities; and data transfers within the EU become unrestricted.

041354 'EU-Richtlinie vor dem Endspurt'

Ulrich Würmeling, *Datenschutzberater v 18 no 12 (15/12/94) pp 1–3 (in German)*

A recent sitting of the ministers responsible for the EU internal market has brought European data protection guidelines significantly nearer. They might be enacted by the middle of 1995. UK objections to its application to manual file systems have mollified by a decision that the official English translation of 'Akten' shall be 'file systems' rather than 'files'.

041355 'Computer Viruses — Legal Options'

BP Zajac, *Network Security (Feb 94) pp 9–10*

The USA has no case law dealing with computer viruses yet. If a virus is caught from shrink-wrapped software, then remedies may be complicated by license disclaimers. The argument would turn on whether these were overly broad.

041356 'The BT hack and what it means'

BP Zajac, *Computer Law and Security Report v 15 no 1 (Jan/Feb 95) pp 35–36*

This article describes an incident in which a UK newspaper got hold of the ex-directory telephone numbers of VIPs, and discusses the apparent lack of security at British Telecom.

041357 'US digital telephony legislation'

BP Zajac, *Computer Law and Security Report v 14 no 6 (Nov/Dec 94) pp 322-323*

Proposed US legislation will force telecomms carriers to provide monitoring capabilities to the government, and is likely to be passed before the next Congressional elections in 1995.

4 Formal Methods and Protocols

041401 'Valuation of Trust in Open Networks'
T Beth, M Borcherding, B Klein, *ESORICS 94 pp 3–18*

The authors develop the formal techniques of **032433** for analysing trust relationships in chains of authentication servers, where various entities may be relied on to generate keys, keep time, keep secrets, identify users and so on. The inference rules for relying on recommendations are based on Bayesian probability.

041402 'Towards Acceptable Key Escrow Systems'
T Beth, HJ Knobloch, M Otten, GJ Simmons, P Wichmann, *Fairfax 94 pp 51–58*

The authors present an alternative key escrow system. This is a Diffie Hellman variant in which the network provides a nonce for use in the generation of each session key. Once an intercept warrant is granted, the investigator takes over this process and with the help of secrets provided by the escrow agent is able to force the two parties to generate weak keys. One effect is that backdated warrants cannot be enforced.

041403 'Secure Wireless LANs'
V Bhargavan, *Fairfax 94 pp 10–17*

The author discusses a number of cryptographic protocols for supporting wireless LAN traffic. The added security requirement in this application is location privacy — an opponent should not be able to find a given machine — and the management of handoff as a mobile moves from one cell to another. He provides a verification of this protocol in the BAN logic.

041404 'A Smartcard Fault-tolerant Authentication Server'
L Blain, Y Deswarte, *Cardis 94 pp 149–165*

The authors report a project to develop a distributed authentication server implemented in smartcards held at different sites by different administrators. The protocols are based on broadcast; authentication requests are broadcast, and the results are combined in various ways. They will resist failures at a certain number of the sites, and have been implemented as part of an ESPRIT project.

041405 'Protocol Failure in the Escrowed Encryption Standard'
M Blaze, *Fairfax 94 pp 59–67*

The author reports a number of attacks on the protocols of the Clipper chip. There are many options available when constructing rogue applications which operate only with each other: one can obscure the LEAF, send it out of band, or even generate it at both ends. However, there is also a way for a rogue application to operate with a genuine one — forward search. This involves trying out random LEAFs on a chip offline until one is found whose 16-bit checksum passes muster for the session key and IV in use. This was tested on an EES PCMCIA card, and usable but bogus LEAFs were found in about 42 minutes on average. Finally, possible fixes are discussed.

041406 'Specification and Validation of a Security Policy Model'
A Boswell, *IEEE Transactions on Software Engineering v 21 no 2 (Feb 95) pp 63–68*

The author describes the development of a security policy model in Z for NATO's Air Command and Control System (ACCS). This has mandatory and discretionary aspects, drawn from both the Bell-LaPadula and Clark-Wilson models, and comprised over 65 schemes. It was validated manually, and was felt to be as large a system as could be dealt with in this way.

041407 'Design and Analysis of Key Exchange Protocols via Secure Channel Identification'
C Boyd, WB Mao, *Asiacrypt 94 pp 149–159*

The authors suggest a new approach to verifying cryptographic protocols; each public key encryption operation creates a channel with either confidentiality or integrity. By writing these as arrows and diagram chasing, it can be seen for example that the TMN protocol is flawed.

041408 'Designing Secure Key Exchange Protocols'
C Boyd, WB Mao, *ESORICS 94 pp 93–105*

The authors present a new protocol formalism which is designed to assist the designer in determining the functional requirements and then translating these into a verified design.

041409 'Formal Methods reality Check: Industrial Usage'
D Craigen, S Gerhart, T Ralston, *IEEE Transactions on Software Engineering v 21 no 2 (Feb 95) pp 90–98*

The authors survey twelve cases of the industrial use of formal methods. These include a firewall and a smartcard system, as well as a number of transport projects and software products.

041410 'Probabilistic Authentication Analysis'
J Domingo-Ferrer, *Cardis 94 pp 49–59*

The author describes a version of the BAN logic in which initial beliefs have probabilities not equal to 0 or 1. Rules for combining probabilities are given, and it is claimed that this approach can help measure the efficiency of cryptographic protocols.

041411 'A Ket Distribution Method for Object-Based Protection'
W Ford, MJ Wiener, *Fairfax 94 pp 193–197*

The authors discuss various ways in which cryptographic keys can be bound into access control blocks for use in distributed systems, especially of the object oriented variety.

041412 'New Protocols for Third-Party-Based Authentication and Secure Broadcast'
L Gong, *Fairfax 94 pp 176–183*

The author presents a number of authentication protocols which use hash functions and Shamir's secret sharing scheme instead of conventional block encryption. The basic idea is that a server who shares different secrets with Alice and Bob can construct some numbers using nonces supplied by them which enable each of them to extract a secret key using polynomial interpolation.

041413 'IRC and Security — Can the Two Co-exist?'
S Gordon, *Network Security (Oct 94) pp 10–17*

This article explains the Internet Relay Chat protocol and describes some of the ways it can be exploited or attacked, including netsplits, robot sessions, collisions, floods and the commoner Trojans.

041414 'Nothing is the Key to the Future'
W Hancock, *Network Security (Oct 94) pp 8–9*

A large number of communications protocols are now having to be reengineered to provide more namespace, since no-one thought that networks would grow as fast as they did. This creates a lot of opportunities for chaos and disruption.

041415 'Beacon Based Authentication'
A Jiwa, J Seberry, YL Zheng, *ESORICS 94 pp 125–141*

The authors develop an idea of Rabin's for a beacon, a service which continually broadcasts certified nonces, and shows that it can be used to simplify authentication protocols. In particular, less messages are needed than with protocols based on user chosen nonces.

041416 'A security model for ISDN using trusted key distribution and authentication'
TK Kwon, JS Song, *JW-ISC 95 pp 191–200*

This paper presents a model for enforcing confidentiality in ISDN, including a policy for confidentiality, a protocol stack on the user-network interface, and a trusted key distribution protocol.

041417 'Endorsements, Licensing, and Insurance for Distributed System Services'
C Lai, G Medvinsky, BC Neuman, *Fairfax 94 pp 170–175*

The authors discuss a number of mechanisms for the endorsement of one security sensitive service by another. In addition to acting as a delivery mechanism for licensing and insurance services, these mechanisms might also be helpful in assessing the risk in using a particular server.

041418 'Delegation keys'
KY Lam, D Gollmann, *Cirencester 93 pp 243–250*

The authors discuss the problems of delegation in distributed systems and the functional requirements for delegation protocols, in the particular context of SPX. They propose that programs to which a user delegates a privilege should have secret keys which are partially dependent on the program name and the user's key, but in a one-way fashion so that user keys cannot be deduced.

041419 'Collision-freedom, considered harmful, or how to boot a computer'
TMA Lomas, *JW-ISC 95 pp 35–42*

In certain circumstances, collision-rich hash functions are more desirable than collision-free ones. This paper shows how collision-rich hash functions have applications in key negotiation, and in a boot protocol for networked workstations.

041420 'A note on supplying a trusted clock via a secure device'
MH Looi, WJ Caelli, *Computers and Security v 13 no 7 (94) pp 611–613*

The authors propose a protocol for updating a clock in a secure device from a trusted master clock which prevents replay attacks (but not delay attacks).

041421 'Anonymous Credit Cards'
SH Low, NF Maxemchuk, S Paul, *Fairfax 94 pp 108–117*

The authors propose a set of protocols for supporting anonymous electronic credit cards. The basic idea is that each user has accounts at two (possibly virtual) banks — one which knows him and is thus prepared to extend credit, and another which does not and which merely handles debit transactions.

041422 'On Strengthening Authentication Protocols to Foil Cryptanalysis'
WB Mao, C Boyd, *ESORICS 94 pp 193–204*

The authors consider how cryptographic protocols might be designed so as to minimise the quantity of known plaintext which they make available to an opponent. They point out that large quantities of known plaintext can be collected by active attacks on protocols such as Kerberos; they recommend that security servers should remember previous runs of protocols; and they propose specific modifications to KryptoKnight.

041423 'On the use of encryption in cryptographic protocols'
WB Mao, C Boyd, *Cirencester 93 pp 251–262*

The authors show that a number of cryptographic protocols, including ISO 9798-2, can be attacked by cut-and-paste techniques if they are implemented using cipher block chaining in such a way that protocol element boundaries coincide with cipher block boundaries.

041424 'A Calculus for Secure Channel Establishment in Open Networks'
UM Maurer, PE Schmid, *ESORICS 94 pp 175–192*

The authors introduce a new notation to help visualise the security relationships in a network: $A \rightarrow\!\bullet B$ means that A can send a secret message to B, while $A \bullet\!\!\rightarrow B$ means that A can send an authentic message to B. They develop a set of formal rules and show that, under reasonable assumptions, $\rightarrow\!\bullet$ is equivalent to $\leftarrow\!\bullet$. Thus one can see at a glance whether it is possible to set up a confidential or authenticated channel between two nodes in a network, by looking for a path between them in which the bullets are all at the same end.

041425 'Formal Verification of Cryptographic Protocols: A Survey'
CA Meadows, *Asiacrypt 94 pp 117–130*

The author gives an overview of the formal techniques used to analyse crypto protocols. She covers state machine methods, such as Millen's Interrogator and the NRL Protocol Analyser, both based on the Dolev-Yao model; modal logics such as BAN; and algebraic approaches such as those of Merritt and Toussaint. She discusses the problems of protocol idealisation and of model granularity, and considers how formal methods can be used in the design phase to clarify requirements.

041426 'Application Access Control at Network Level'
R Molva, E Rütschke, *Fairfax 94 pp 219–228*

The authors discuss a mechanism whereby applications use a secure protocol stack to insert precomputed tickets into packets, and any packets without them are killed at a firewall. This enables network layer enforcement of application level security policies. An implementation in IP is described; it is suggested that mechanisms of this kind are ideal for securing multicast channels, especially against flooding attacks.

041427 'Prerequisite Confidentiality'
JP Nestor, ES Lee, *Fairfax 94 pp 282–293*

The authors propose a new definition of confidentiality in multilevel systems, which is based on formal modelling by event systems and deterministic regular parsable grammars. The goal is to build a structure in which composability can be dealt with in a coherent and rigorous manner. Like Lin's behavioural security model, it is based on input-output causality and requires that high-level input events never be prerequisites for low-level output events.

041428 'Secure Agreement Protocols: Reliable and Atomic Group Multicast in Rampart'
MK Reiter, *Fairfax 94 pp 68–80*

The author presents new protocols which ensure that all honest members of a group deliver the same messages in the same order, and describes their implementation in a toolkit for building high-integrity distributed services. They are based on the author's secure group membership protocol, and the basic building block is echo multicast: a single member publishes a message — sends it to all group members — gets their answers, and publishes these too. It thus gets round the traditional problem of telling whether a group member is dishonest or merely unreachable, and therefore makes secure multicast protocols feasible in loosely-coupled asynchronous systems. Performance measurements for a trial implementation are given.

041429 'A Consideration of the Modes of Operation for Secure Systems'
CL Robinson, SR Wiseman, *ESORICS 94 pp 335–356*

The authors examine the UK's modes of system operation (dedicated, system high, compartmented and multilevel) and present of formal model in Z of the underlying rules. This was of benefit because it forced the authors to examine the difficult aspects of the problem, which would have otherwise been avoided, and to come up with succinct definitions.

041430 'Protocols that ensure fairness'
GJ Simmons, *Cirencester 93 pp 383–394*

The Diffie Hellman protocol contains a number of potentially unfair aspects. For example, either party can force the key to be a multiple of a particular factor of $p-1$. Although these do not give rise to practical attacks in Diffie Hellman, the same principles can be used to construct subliminal channels in discrete log based signature schemes. In particular, a variant of DSS in which session keys are chosen interactively with authority suffers from a 'cuckoo's channel': authority can force the choice of key so as to hide information. The author concludes with a principle for protocol design: 'don't trust anything that you can't enforce or verify'.

041431 'On key agreement protocols based on tamper-proof hardware'
YL Zheng, *Information Processing Letters v 53 no 1 (13/1/95) pp 49–54*

The author breaks a key escrow protocol proposed by Leighton and Micali at Crypto 93, which was based on repeated hashing in secure hardware. By feeding suitably chosen information into her chip, a user can recover a key shared by two other participants.

5 Secret Key Algorithms

041501 'Cryptanalysis of Multiple Modes of Operation'
E Biham, *Asiacrypt 94 pp 230–245*

This paper analyses the security of multiple modes of operation of a block cipher. For example, if we wish to use triple DES and CBC, should we apply single DES in CBC mode three times, or use the CBC mode of the block cipher obtained by applying DES three times? It is shown that the former is significantly less secure — in fact, it is only slightly stronger than the CBC mode of single DES — and similar attacks apply to many other exotic modes. The basic idea is to look for the shortest path through the cipher, and the moral is to apply the standard modes of operation to a block cipher consisting of multiple encryption.

041502 'How To Strengthen DES Using Existing Hardware'
E Biham, A Biryukov, *Asiacrypt 94 pp 339–353*

Some hardware implementations of DES allow the loading of arbitrary S-boxes, and this paper describes how these S-boxes could be made key dependent without affecting the resistance to known cryptanalytic attacks. The resulting cipher has a key of 112 bits, which makes exhaustive key search infeasible, and is claimed to be at least as resistant as DES to linear, differential and other attacks.

041503 'How to Break Gifford's Cipher'
TR Cain, AT Sherman, *Fairfax 94 pp 198–209*

The authors describe a stream cipher based on a nonlinear filter generator which was used to encrypt newswire traffic in the 1980's. They show that, since the underlying shift register is not irreducible, its state space can be factored into subspaces, of which the largest has 2^{40} elements. Given that the plaintext was ASCII, every eight bit of keystream is known, so there is a keysearch attack taking 2^{40} steps. They then show a time-space tradeoff which cuts the work factor to 2^{27} trials, given 2^{18} bytes of memory. A production attack takes four hours on eight Sparcstations.

041504 'Attacking the SL_2 Hashing Scheme'
C Charnes, J Pieprzyk, *Asiacrypt 94 pp 268–276*

The authors produce a collision for Tillich and Zémor's hash function, which was based on $SL_2(2, 2^n)$ and introduced at Crypto 94 (**034545**). The attack is restricted to the values of n for which either $2^n - 1$ or $2^n + 1$ has a small prime factor.

041505 'Semi-bent Functions'
ST Chee, SJ Lee, KJ Kim, *Asiacrypt 94 pp 84–95*

The authors study balanced functions of n input bits with relatively high nonlinearity. They also show that this class contains functions that satisfy the propagation criterion of order $n-1$. They call two Boolean functions f and g strictly uncorrelated if f, g and $f \oplus g$ are all balanced and satisfy a propagation criterion of order 1. Finally, they exhibit semi-bent functions which are strictly uncorrelated.

041506 'On polynomial functions from Z_n to Z_m'
ZB Chen, *Discrete Mathematics v 137 (20/1/95) pp 137–145*

If n is not greater than the smallest prime factor of m, then all functions from Z_n to Z_m are polynomial, and there is a unique such polynomial with small coefficients.

041507 'The Lorenz Cipher Machine SZ42'
DW Davies, *Cryptologia v XIX no 1 (Jan 95) pp 39–61*

The author describes the Lorentz Shlüsselzusatz, which was broken at Bletchley using Colossus. He gives diagrams for the electrical circuitry, the wheel driving and cam mechanisms, and the timing, based on the machine in the crypto museum at Bletchley.

041508 'Analogue pseudorandom sequences for communication applications'
M Darnell, *Cirencester 93 pp 121–139*

The author considers how q-ary m-sequences can be used to provide analogue keystreams for spread spectrum applications, and in particular the effect on them of signal processing operations such as preemphasis, deemphasis and integration.

041509 'Pairs and Triplets of DES S-Boxes'
D Davies, S Murphy, *Journal of Cryptology v 8 no 1 (1995) pp 1–25*

The input to any pair of adjacent DES S-boxes is constrained by two bits of information about the key, and the eight-bit output of the two boxes is not a uniform function of these bits. This, plus the fact that known plaintext gives the xor of eight instances of the round function, gives a statistical attack on DES; but about 2^{52} known plaintexts would be needed, which is worse than for linear cryptanalysis. One complication is that one can design ciphers which, like DES, resist this kind of attack, but which are vulnerable to attacks based on triplets of S-boxes.

041510 'Simultaneous correlation to many linear functionals: a new cryptanalytic technique which can almost halve the key size of certain stream ciphers'
MW Dodd, *Cirencester 93 pp 141–158*

A Boolean function is completely characterised by its correlations to all linear functions, and this leads to a number of results including various expressions for the unicity distance of a stream cipher. Attacks using simultaneous correlations may use less keystream than those based on a single correlation.

041511 'Five New Orders for Hadamard Matrices of Skew Type'
DŽ Doković, *Australasian Journal of Combinatorics v 10 (Sep 94) pp 289–294*

The author exhibits Hadamard matrices of order $4n$ for $n = 81{,}103$, 151, 169 and 463.

041512 'On the discrepancy of quadratic congruential pseudorandom numbers with power of two modulus'
J Eichenauer-Herrmann, *Journal of Computational and Applied Mathematics v 53 (94) pp 371–376*

A positive fraction of maximal length quadratic sequences over $GF(2^n)$ have a discrepancy of at least $O(2^{n/3})$.

041513 'Orthogonal complementary sets of sequences'
PZ Fan, M Darnell, B Honary, *Cirencester 93 pp 183–193*

The authors present some new methods for synthesising mutually orthogonal sequences. They show that there are many more orthogonal complementary sets than uncorrelated complementary sets, and make a number of conjectures.

041514 'On the linear complexity of nonlinearly filtered PN-sequences'
A Fúster-Sabater, P Caballero-Gil, *Asiacrypt 94 pp 61–71*

The authors provide a general lower bound on the linear complexity of nonlinearly filtered sequences, and an algorithm to improve it in specific cases. Unlike Rueppel's root presence test, their technique is based on analysing binary patterns rather than determinants, and is independent of the underlying shift register.

041515 'Pseudo random permutation generators for DSP implementation of analogue signals scrambling'
SC Goh, SM Park, SJ Lee, *JW-ISC 95 pp 85–93*

The authors propose two cryptographic sequence generators: one is based on the linear congruential generator, and the other on the quadratic congruential generator.

041516 'Intrinsic Weakness of Keystream Generators'
JD Golić, *Asiacrypt 94 pp 72–83*

If an arbitrary keystream generator has M bits of state, then there is a linear function of at most $M+1$ bits $k_t, ...k_{t+M}$ which is an unbalanced function of the initial state and whose probability distribution is independent of t if the next-state function is balanced. This can be used as the basis for linear approximation attacks, which are discussed in the case of several generators.

041517 'Three Characterisations of Non-Binary Correlation-Immune and Resilient Functions'
K Gopalakrishnan, DR Stinson, *Designs, Codes and Cryptography v 5 no 3 (May 95) pp 241–251*

The authors generalise the Xiao-Massey lemma to the case of odd characteristic, and use it to characterise t-th order correlation immune and resilient functions of n variables over $GF(q)$. There are three equivalent forms of this: in terms of a matrix of incidence probabilities, a sum of roots of unity, and a set of orthogonal arrays.

041518 'Linear dependencies in product ciphers'
HM Gustafson, AW Pettitt, EP Dawson, LJ O'Connot, *Australasian Journal of Combinatorics v 10 (Sep 94) pp 115–129*

The authors survey the various kinds of linear dependency which a block cipher can exhibit and which make it vulnerable to differential, linear and other attacks. They show that these dependencies are very unlikely to occur in a random cipher.

041519 'On the Security of the CAST Encryption Algorithm'
HM Heys, SE Tavares, *Proceedings of the Canadian Conference on Electrical and Computer Engineering, September 94, Halifax*

The authors further describe the CAST algorithm used in North American digital cellular telephones, and whose principles were first described in **022501**. It is a Feistel cipher with a round function of four 8 by 32 bit S-boxes, whose outputs are x-ored together. Various results on resistance to linear, differential and related-key analysis are given.

041520 'The Design of Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis'
H Heys, S. Tavares, *Fairfax 94 pp 148–155*

A scheme for a block cipher is proposed based on the substitution-permutation networks which were proposed by Feistel in the early seventies. The authors derive upper bounds on the probability of the best characteristic and of the best linear approximation. They conclude that large S-boxes with good diffusion properties increase the resistance to differential cryptanalysis, and that linear transformations between the rounds can increase the resistance to linear cryptanalysis.

041521 'How to strengthen DES against two robust attacks'
K Kim, S Lee, S Park, D Lee, *JW-ISC 95 pp 173–182*

The authors propose an alternate set of DES S-boxes which are claimed to be more secure against both linear and differential cryptanalysis.

041522 'Classification of Hadamard matrices of order 28'
H Kimura, *Discrete Mathematics v 133 (Oct 94) pp 171–180*

The author classifies all Hadamard matrices of order 28. Those with trivial K-matrices correspond to the squares in $GF(27)$.

041523 'A model for secret-key cryptography using chaotic synchronisation'
L Kocarev, T Stojanovski, *ISITA 94 pp 251–255*

A new application of the concept of chaotic synchronization to secure communication systems is proposed. This is a chaotic system which takes the information signal as an input and produces an output that can be decoded in the receiver to reconstruct the information signal without error. Statistical measurements of the performance of the system are reported.

041524 'Multiplication of sequences with zero autocorrelation'
C Koukouvinos, S Kounias, J Seberry, CH Yang, J Yang, *Australasian Journal of Combinatorics v 10 (Sep 94) pp 5–16*

The authors exhibit near normal sequences of new lengths 49, 53 and 57. Golay sequences can be constructed from sequences of this type.

041525 'An efficient method to find the linear expressions for linear cryptanalysis'
S Lee, SH Sung, K Kim, *JW-ISC 95 pp 183–190*

The authors propose an algorithm for determining effective linear expressions for linear cryptanalysis; its search time is independent of the number of rounds.

041526 'Free energy minimisation algorithm for decoding and cryptanalysis'
DJC MacKay, *Electronics Letters v 31 no 6 (16/3/95) pp 446–447*

The author tackles the problem of shift register reconstruction in a general context. He provides an algorithm to infer a binary vector s given noisy observations of As (mod 2), where A is a binary matrix; s is replaced by a vector of probabilities, and free energy minimisation techniques drawn from statistical mechanics are used. The algorithm performs better than previous reconstruction techniques: it gives solutions right up to the Meier Staffelbach bound.

041527 'Recent topics on block ciphers–open problems to be solved'
M Matsui, *JW-ISC 95 pp 239–243*

This paper presents two open problems concerning differential and linear cryptanalysis: the lower bound of the two parameters differential uniformity and nonlinearity, and algorithms for searching for finding good multiple differential or linear paths.

041528 'Short Gollmann cascade generators may be insecure'
R Menicocci, *Cirencester 93 pp 281–297*

The Gollmann generator, which is a cascade of stop-go shift registers with feedforward, has the property that the output of each stage is correlated 50% with that of the previous stage. Thus a correlation of 2^{-L} can be obtained between a keystream and the first in a cascade of L shift registers.

041529 'A Correlation Attack on the Binary Sequence Generators with Time-Varying Output Function'
MJ Mihaljević, *Asiacrypt 94 pp 49–60*

By counting the number of times a bit in one sequence agrees with the bits in a segment of another sequence, one obtains a novel distance measure which can be used to construct a correlation attack a number of stream ciphers, including MacLaren-Marsaglia type systems, multilexer generators

041530 'Novel tests for the security examination of pseudorandom bit generators'
MJ Mihaljević, *ISITA 94 pp 277–282*

The author proposes two new statistical tests to measure the resistance of pseudorandom bit generators against correlation attacks. Each ensures resistance against a particular type of correlation attack, and they are both more efficient than the corresponding attacks. Hence they can be used in practice to measure resistance against these attacks.

041531 'The Cryptographic Mathematics of Enigma'
AR Miller, *Cryptologia v XIX no 1 (Jan 95) pp 65–80*

The author describes the Enigma and calculates the effective key diversity of a number of configurations.

041532 'New c-ary perfect factors in the de Bruijn graph'
CJ Mitchell, *Cirencester 93 pp 299–313*

A perfect factor is a set of cycles whose elements are drawn from some set and such that each n-tuple occurred exactly once — a generalisation of a de Bruijn sequence. These are further generalised by the author to structures which contain each tuple within a given segment of one of the sequences; some constructions are given, and this provides some perfect factors of previously unknown size.

041533 'Aperiodic and Semi-Periodic Perfect Maps'
CJ Mitchell, *IEEE Transactions on Information Theory v 41 no 1 (Jan 95) pp 88–95*

The author constructs aperiodic and semi-periodic perfect maps for all possible parameter sets, and thus shows that they exist even where periodic ones do not.

041534 'A study on the security of RDES-1 cryptosystem against linear cryptanalysis'
Y Nakao, T Kaneko, K Koyama, R Terada, *JW-ISC 95 pp 163–172*

RDES-1 is a variant of DES in which a probabilistic swapping function is added onto the right half of the input to each round. It is shown to be more secure than DES against linear cryptanalysis.

041535 'On a new factorisation algorithm for polynomials over finite fields'
H Niederreiter, R Göttfert, *Mathematics of Computation v 64 no 209 (Jan 95) pp 347–353*

The first author's polynomial factorisation algorithm was improved by the second for the case of characteristic two. They now join forces to optimise it for arbitrary positive characteristic.

041536 'Provable Security Against a Differential Attack'
K Nyberg, LR Knudsen, *Journal of Cryptology v 8 no 1 (1995) pp 27–37*

The authors prove lower bounds on the differentials of block cipher round functions given by quadratic permutations, and exhibit one of the form x^{2^k+1} for which the maximum probability is 2^{3-n}, where n is the block size. They also show bounds on multiround probabilities. Finally, they suggest using x^3 in $GF(2^{33})$, with one output coordinate discarded, as a round function. With six rounds, and 198 independent key bits, this should have a maximum differential probability of 2^{-61}.

041537 'An upper bound on the number of functions satisfying the strict avalanche criterion'
L O'Connor, *Information Processing Letters v 52 no 6 (23/12/94) pp 325–327*

The author defines $S(n,k)$ as the number of Boolean functions on n variables which are 50% dependent on any subset of k variables. He provides closed form expressions for $S(n,1)$ and $S(n,2)$, and an inequality between $S(n,k)$ and the number of functions satisfying a strict avalanche criterion of order k.

041538 'A Unified Markov Approach to Differential and Linear Cryptanalysis'
L O'Connor, JD Golić, *Asiacrypt 94 pp 328–338*

This paper introduces Markov methods to linear cryptanalysis, as Lai, Massey and Murphy did for differential cryptanalysis. Based on results in random graph theory, it is shown that if the round function of an iterated block cipher is a random function, both Markov chains converge to the uniform distribution with high probability under the assumption that the rounds are independent uniformly distributed random variables.

041539 'Simple permutation ciphers using permutation polynomials'
E Okamoto, W Aiken, GR Blakely, PF Stiller, *ISITA 94 pp 239–244*

In this paper, polynomials over finite fields that induce a permutation on the elements of the field are considered. The application of these polynomials to construction of permutation ciphers is studied, and security of the resulting systems is analysed.

041540 'Collisions and Inversions for Damgård's Whole Hash Function'
J Patarin, *Asiacrypt 94 pp 257–267*

The author extends his algebraic approach to attack hash functions based on the knapsack problem. Previously this had been able to find collisions or preimages for the round function; now a collision or preimage for the hash function itself can be computed, and the algorithm is compared to lattice basis reduction attacks. The author also proposes an improved hash function.

041541 'Enumerating perfect maps'
KG Paterson, PR Hoare, *Cirencester 93 pp 327–339*

Perfect maps are the two-dimensional analogue of De Bruijn sequences — each subarray of a given size occurs exactly once. Graph theoretic constructions can be used to give lower bounds on the numbers of such objects.

041542 'Cryptographic Boolean functions via group Hadamard matrices'
J Seberry, XM Zhang, YL Zheng, *Australasian Journal of Combinatorics v 10 (Sep 94) pp 131–145*

The authors show how to use Hadamard matrices to c9onstruct sets of highly nonlinear, balanced multipermutations from n to m bits for $2m < n < m$ which also satisfy the strict avalanche criterion.

041543 'Structure of highly nonlinear cryptographic functions'
J Seberry, XM Zhang, YL Zheng, *ISITA 94 pp 229–234*

In this paper, cryptographic properties of of non-linear Boolean functions are investigated, and in particular the relation between non-linearity and propagation properties. The main result of the paper is a characterisation of functions that satisfy propagation criteria with respect to all but at most 6 vectors.

041544 'Structures of Cryptographic Functions with Strong Avalanche Characteristics'
J Seberry, XM Zhang, YL Zheng, *Asiacrypt 94 pp 96–106*

Boolean functions are studied which satisfy the propagation criterion for all but a small set of vectors, denoted with $\mathcal{R}$. It is shown that if $|\mathcal{R}|> 2$, the non-zero vectors in such a set have to be linearly dependent. Also, there are no functions with $|\mathcal{R}|= 3$ or 6. For $|\mathcal{R}|= 2, 4, 5$ the non-linearity is calculated, and the linear structures are identified.

041545 'Non-Abelian Hadamard Difference Sets'
KW Smith, *Journal of Combinatorial Theory Series A v 70 no 1 (Apr 95) pp 144–156*

Difference sets with parameters $(4t^2, 2t^2 - t, t^2 - t)$ may exist even where there are no such Abelian sets; an example is given where the underlying group is of order 100 and $t= 2^q.3^r.5.10^s$.

041546 'How to strengthen FEAL against differential cryptanalysis'
R Terada, GG Pinheiro, *JW-ISC 95 pp 153–162*

This paper presents a variant of FEAL-N(X), called FEAL-N(X)S, which adds a dynamic swapping function after each round. It is claimed to be stronger against differential cryptanalysis than FEAL-N(X), with a decrease in performance of only 10%.

041547 'Linear Cryptanalysis of LOKI and s^2DES'

T Tokita, T Sorimachi, M Matsui, *Asiacrypt 94 pp 246–256*

The authors apply Matsui's branch and bound algorithm to find the best characteristics and linear approximations for LOKI89, LOKI91, and to s^2DES (a DES variant with modified S-boxes). They conclude that n rounds of LOKI89 and LOKI91 seem to achieve the same resistance as $2n$ rounds of DES to differential and linear attacks.

041548 'Parallel Collision Search with Application to Hash Functions and Discrete Logarithms'

P Van Oorschot, M Wiener, *Fairfax 94 pp 210–218*

The authors present a parallel version of Pollard's ρ-method; this could be used in a $10 million collision search machine which would find collisions for a hash function like MD5 in 24 days. The same algorithm can also be applied to find discrete logarithms in an elliptic curve group where the largest prime factor of the order of the elliptic curve group is relatively small (128 bits).

041549 'Maximum Correlation Analysis of Nonlinear Combining Functions'

GZ Xiao, MX Zhang, *Asiacrypt 94 pp 107–116*

The authors study the maximum correlation between a Boolean function and the set of all Boolean functions of a subset of its inputs. An efficient procedure is proposed to compute a maximum correlator for the case of balanced Boolean functions, and it is shown that this results in an improved correlation attack on a combination generator. Also, the maximum correlation is computed for bent functions.

041550 'Correlation-immune random sequence generator using GMW sequences'

HY Youm, MY Rhee, *JW-ISC 95 pp 67–84*

This paper examines the properties of random sequences generated by nonlinear functions, and proposes a new random sequence generator based on the GMW sequences which is highly correlation immune. The structure of this generator is examined, and its linear complexity and period are analyzed.

041551 'Information Leakage of Boolean Functions and its Relationship to Other Cryptographic Criteria'

M Zhang, S Tavares, L Campbell, *Fairfax 94 pp 156–165*

The paper uses an information theoretic approach to define new criteria for Boolean functions; these are related to existing criteria such as nonlinearity, resilience, and higher order avalanche criteria.

6 Public Key Algorithms

041601 'A Digital Signature Scheme Based on Linear Error-Correcting Block Codes'
M Alabbadi, SB Wicker, *Asiacrypt 94 pp 197–207*

The authors presented a digital signature scheme based on linear error-correcting codes (which was broken by Stern at the rump session).

041602 'Combined data encryption and reliability using McEliece's public-key cryptosystem'
M Alabbadi, S Wicker, *ISITA 94 pp 263–268*

This paper explores a series of modifications to McEliece's public key cryptosystem that provide error detection and correction capability at the cost of reduced security.

041603 'The classification of hash functions'
RJ Anderson, *Cirencester 93 pp 83–93*

The author examines the properties which hash functions must have in order not to interact with digital signature schemes in a dangerous manner. He shows that collision freedom is not enough by proving Okamoto's conjecture that correlation freedom is a strictly stronger property, and then shows that no set of constructive freedom properties would be adequate for a hash function to be used with a signature scheme of Yen and Laih. He concludes that it is prudent to specify hash function properties explicitly in each individual case.

041604 'Secure Acceleration of DSS Signatures using Insecure Server'
P Béguin, JJ Quisquater, *Asiacrypt 94 pp 208–218*

A method is presented for a slow processor (such as a smart card) to compute a modular multiplication and exponentiation with the aid of an untrusted server. The protocol requires no precomputation by the slow processor, and is claimed to be secure against both active and passive attacks. For practical parameters, a speedup with a factor between 3 and 4 is achieved.

041605 'The ESPRIT Project CAFE — High Security Digital Payment Systems'
JP Boly, A Bosselaers, R Cramer, R Michelsen, S Mjølsnes, F Muller, T Pedersen, B Pfitzmann, P de Rooij, B Schoenmakers, M Schunter, L Vallée, M Waidner, *ESORICS 94 pp 217–230*

The authors describe project CAFE, a European initiative to create an electronic purse for low-value anonymous payments. This is based on a user device with a tamper resistant guardian (in a smartcard supplied by the bank) and protocols to detect double spending if the tamperproofing is defeated. Unlike some other systems, it will support multiple currencies; it will also provide loss tolerance in that users can make backups of their digital money. It is claimed to provide a high degree of legal certainty in the event of disputes.

041606 'Off-Line Cash Transfer by Smart Cards'
S Brands, *Cardis 94 pp 101–117*

The author presents an electronic cash system, which is based on using a machine such as a PC (which is supplied by the user but not trusted by the bank) to do as much of the computation as possible, leaving only a single modular multiplication to be done online by the guardian, a bank issued smartcard with a counter. If the tamper protection on a card is broken, the exposure can still be controlled in various ways.

041607 'An Efficient Electronic Payment System Protecting Privacy'
JL Camenisch, JM Piveteau, MA Stadler, *ESORICS 94 pp 207–215*

The authors propose a payment system based on anonymous accounts; customers can set up new accounts under pseudonyms, and transfer money between accounts under their control. This gives most of the practical advantages of digital cash, without requiring the bank to store large amounts of data on coins in issue.

041608 'Conditionally Secure Secret Sharing Schemes with Disenrollment Capability'
C Charnes, J Pieprzyk, R Safavi-Naini, *Fairfax 94 pp 89–95*

The authors describe a variant of Shamir's secret sharing scheme, which has been given a disenrollment capability. Users have two shadows related by discrete logarithm modulo a Mersenne prime.

041609 'Oblivious Signatures'
LD Chen, *ESORICS 94 pp 161–172*

Two signature schemes are proposed. In one of them, the recipient can choose to get one message out of n signed, and in the other she can choose to get a message signed with one out of n keys; in neither case will be signer know which was chosen. Both of these schemes are quite efficient and are based on the Chaum-Pedersen signature scheme.

041610 'Optimisation, fitness and the knapsack cipher'
A Clark, E Dawson, H Bergen, *ISITA 94 pp 257–261*

This paper considers applying combinatorial optimization to cryptanalysis, and in particular, using simulated annealing, genetic algorithms or tabu search to breaking knapsack ciphers. The conclusion is that such techniques are not suitable for large knapsacks; although the search space might be reduced, they are slower in practice than the alternatives.

041611 'On public-key cryptosystems based on linear codes: efficiency and weakness'
EM Gabidulin, *Cirencester 93 pp 17–31*

The author had proposed a public key cryptosystem based on rank codes, but it was broken by Gibson. In this paper, he proposes a modification which is claimed to defeat the attack.

041612 'Modified key agreement protocol based on the digital signature standard'
L Harn, *Electronics Letters v 31 no 6 (16/3/95) pp 448–449*

The author proposes a Diffie Hellman variant with inbuilt DSS authentication. It avoids the Nyberg-Rueppel attack by exchanging two keys at once and signing their sum.

041613 'Meta-ElGamal signature schemes'
P Horster, H Petersen, M Michels, *Fairfax 94 pp 96–107*

The authors systematically enumerate a number of variants of the ElGamal signature scheme. They present a total of thirty variants, a similar number of schemes for signing two messages at once, and six schemes for three messages. A similar analysis for DSA shows five variants which are efficient for signature validation and eight which are efficient for verification; only one scheme — already proposed by Nyberg and Rueppel — is common to both of these lists.

041614 'Meta Message Recovery and Meta Blind Signature Schemes Based on the Discrete Logarithm Problem and Their Applications'
P Horster, H Petersen, M Michels, *Asiacrypt 94 pp 185–196*

Existing techniques to add message recovery to El-Gamal based signature schemes can be extended to the more general Meta-ElGamal signature scheme. Blind signature techniques can also be extended.

041615 'On Key Distribution via True Broadcasting'
M Just, E Kranakis, D Krizanc, P van Oorschot, *Fairfax 94 pp 81–88*

The authors present a number of schemes for broadcast key distribution, and provide lower bounds on the size of the key under certain assumptions.

041616 'New sequential and simultaneous multisignature schemes'
CG Kang, DY Kim, DH Kim, DK Lee, *ISITA 94 pp 283–288*

Two new multisignature schemes are proposed, both of which are based on Fiat-Shamir. In one of them, the participants sign the message sequentially, while in the other the message is broadcast to the signers, who individually sign it and return their signatures to the originator for composition. The security and efficiency of the schemes are analysed.

041617 'Conference key distribution protocols in distributed systems'
B Klein, M Otten, T Beth, *Cirencester 93 pp 225–241*

The authors discuss the options for setting up conference keys in distributed systems. They propose two new protocols: a multi-party Diffie Hellman variant with authentication and cheater detection, and a scheme based on secret sharing and multiple servers.

041618 'A new RSA-type scheme based on singular cubic curves'
H Kurakado, K. Koyama, *JW-ISC 95 pp 144–151*

This paper presents a new RSA-type scheme over non-singular parts of singular cubic curves $E_n(a,b)$: $(y-ax)(y-bx) = x^3 \pmod n$.

041619 'Low exponent attack against elliptic curve RSA'
K Kurosawa, K Okada, S Tsujii, *Asiacrypt 94 pp 318–327*

The authors extend Hastad's low exponent attack on RSA to the elliptic curve variants of RSA developed by Demytko and by Koyama, Maurer, Okamoto and Vanstone.

041620 'Group signer/verifier separation scheme'
K Kurosawa, C Park, K Sakano, *JW-ISC 95 pp 134–143*

In many kinds of signature scheme, it is useful to consider not only the relation between the signer and the plaintext, but also the relation between a signature and a signer. This paper illustrates this separation by presenting a scheme in which everyone can verify the relation between the signer and the signature noninteractively, but only an interactive protocol can verify the relation between the signer and the plaintext.

041621 'Authentication and protection of public keys'
CS Laih, WH Chiou, CC Chang, *Computers and Security v 13 no 581–585*

The authors develop Girault's idea of self-certifying public keys (keys with the property that certificate forgery by authority can be proved) to the case where there are multiple authorities, some of whom are dishonest.

041622 'On the security of the Lucas function'
CS Laih, FK Tu, WC Tai, *Information Processing Letters v 53 no 5 (10/3/95) pp 243–247*

The authors show that an oracle for the Lucas function could be used to extract discrete logarithms in polynomial time.

041623 'Efficiency of SS(l) square-and-multiply exponentiation algorithm'
KY Lam, LCK Hui, *Electronics Letters v 30 no 25 (8/12/94) pp 2115–2116*

The authors examine the efficiency of square-and-multiply exponentiation algorithms which use a table of 2^k precomputed values to reduce the effective weight of an n-bit exponent. The weight achieved by such algorithms had been observed empirically to be $n/(l+1)$; this is proved to hold in the limit.

041624 'Comment — digital signature with $9t, n)$ shared verification based on discrete logarithms'
WB Lee, CC Chang, *Electronics Letters v 31 no 3 (2/2/95) pp 176–177; with reply by L Harn*

The authors show how to forge messages for a signature scheme of Harn, who proposes a fix for the problem in an attached reply.

041625 'A dynamic cryptographic key generation and information broadcasting scheme in information systems'
HT Liaw, *Computers and Security v 13 no 7 (94) pp 601–610*

The author proposes a hierarchical key management scheme based on RSA which enables each user to calculate the secret keys in use at lower levels in a lattice.

041626 'A New Public-Key Cipher Based Upon the Diophantine Equations'
CH Lin, CC Chang, RCT Lee, *IEEE Transactions on Computers v 44 no 1 (Jan 95) pp 13–19*

The authors present a knapsack type system which is packaged in Diophantine equation terminology.

041627 'Can Montgomery Parasites be Avoided? A Design Methodology Based on Key and Cryptosystem Modifications'
D Naccache, D M'Raïhe, D Raphaeli, *Designs, Codes and Cryptography v 5 no 1 (Jan 95) pp 73–80*

If everyone is using Montgomery multiplication, then it makes sense to change the definitions of the common cryptographic algorithms slightly so that operand scaling can be dispensed with. The details are set out for a number of popular public key schemes.

041628 'How to prevent buying of votes in computer elections'
V Niemi, A Renvall, *Asiacrypt 94 pp 141–148*

Most electronic voting protocols suffer from the problem that voters can prove which way they voted; this makes it possible for votes to be bought or coerced. The authors had previously proposed a system in which did not possess this property, but which relied on a trusted third party; in this paper, they show how the candidates can use secret sharing and multiparty computation techniques to remove this constraint.

041629 'Secure anonymous channel against active attack'
C Park, K Kurosawa, *JW-ISC 95 pp 15–23*

The authors consider means of countering an attack by Pfitzmann on an anonymous channel.

041630 'An entrusted undeniable signature'
SJ Park, KH Lee, DH Won, *JW-ISC 95 pp 120–133*

The authors propose the concept of an entrusted undeniable signature: the signer can confirm his signature to a verifier without any help, but cannot run a disavowal protocol without the help of a trusted third party (a court). This scheme is constructed by the combination of undeniable signatures and zero-knowledge proofs.

041631 'A public-key cryptosystem and a digital signature scheme based on the Lucas function analogue to discrete logarithms'
P Smith, C Skinner,*Asiacrypt 94 pp 298–306*

The authors propose basing ElGamal schemes on the corational group of $GF(p^2)$, and claim that these are much stronger than systems based on the rational group.

041632 'A Fast Off-line Electronic Currency Protocol for Smart Cards'
L Tang, JD Tygar, *Cardis 94 pp 89–100*

In this article, the authors propose a new electronic cash scheme; however, it was broken at the workshop by Brands.

041633 'Using four-prime RSA in which some of the bits are specified'
SA Vanstone, RJ Zuccherato, *Electronics Letters v 30 no 25 (8/12/94) pp 2118–2119*

The authors propose that when moving from 512-bit to 1024-bit RSA, users should pick four prime factors rather than two for downward compatibility reasons, and claim that over 250 bits of the modulus can be fixed in order to save storage.

041634 'Efficient Extended Money'
Y Yacobi, *Asiacrypt 94 pp 131–140*

The author presents a new digital cash scheme which offers untraceability but not unlinkability of payments by the same user. As a result, it is in many respects simpler than existing systems.

041635 'Cryptanalysis of secure addition chain for SASC applications'
SM Yen, *Electronics Letters v 31 no 3 (2/2/95) pp 175–176*

The author points out a flaw in an addition chain based protocol for server aided secret computation.

7 Computational Number Theory

041701 'The Rabin-Miller primality test: composite numbers which pass it'
F Arnault, *Mathematics of Computation v 64 no 209 (Jan 95) pp 355–361*
The author provides a new technique, based on biquadratic reciprocity, for generating strong pseudoprimes with respect to a given set of bases. He exhibits an integer which is a strong pseudoprime with respect to the first forty six prime numbers.

041702 'The Magic Words Are Squeamish Ossifrage'
D Atkins, M Graff, AK Lenstra, PC Leyland, *Asiacrypt 94 pp 219–229*
The authors describe how they factored the 129-digit RSA challenge which was published in 1977 in Scientific American. They used the double large prime variation of the multiple polynomial quadratic sieve value, and were assisted by the spare cycles of 1600 machines on the Internet. It was discovered that the results of the computation can be approximated by a quartic function of the number of relations received, rather than as a quadratic function as expected. They conclude that 512-bit RSA moduli are vulnerable to any organisation willing to spend a few million dollars and wait a few months.

041703 'On the squared unsymmetric Lanczos method'
AT Chronopoulos, *Journal of Computational and Applied Mathematics v 54 (94) pp 65–78*
The author discusses an optimisation of the Lanczos method for finding eigenvalues of nonsymmetric matrices. Tests on a system of 40,000 equations show it to be competitive and economical of memory.

041704 'Small Zeros of Quadratic Congruences modulo pq, II'
T Cochrane, *Journal of Number Theory v 50 no 2 (Feb 95) pp 299–308*
For $n \geq 4$, the quadratic congruence $Q(x_1, x_2, ..., x_n) \equiv 0 \pmod{pq}$ has a nonzero solution with $\max|x_i| \ll \sqrt{pq}$, and this is the best possible such result.

041705 'Computing $\pi(x)$, $M(x)$ and $\Psi(x)$'
M Deléglise, J Rivat, *ANTS 94 p 264*
The authors report a slight improvement in the Lagarias-Miller-Odlyzko method for calculating $\pi(x)$ — their variant runs a multiple of $O(\log x)$ faster at the cost of a similar increase in memory size.

041706 'On Orders of Optimal Normal Basis Generators'
SH Gao, SA Vanstone, *ANTS 94 p 220*
The authors did a numerical investigation of a large number of optimal normal bases for fields of characteristic 2. Where γ is primitive and $\alpha = \gamma + \gamma^{-1}$ generates the basis, α^e can be computed in $O(n.w(e))$ operations, where $w(e)$ is the Hamming weight of e. If α were an arbitrary value, the cost would be $O(n \log n \log\log n \log e)$ computations.

041707 'The complexity of greatest common divisor computations'
BS Majewski, G Havas, *ANTS 94 pp 184–193*
The authors consider the complexity of expressing the GCD of $n > 2$ numbers as a linear combination of them, and shows that this problem is NP-complete. However, the largest multiplier cannot exceed half the largest input number.

041708 'Parallel decomposition of modular exponentiation for RSA cryptosystem'
S Shimonaka, N Takeda, H Nagase, *ISITA 94 pp 269–271*
The authors propose calculating M^e by decomposing M into factors and raising

each factor to the power e to get a collection of partial results, which can then be combined. Speed-up may be obtained if partial results can be calculated in parallel and/or with the aid of a stored table. Experimental results on performance are reported.

041709 'Still faster modular multiplication'
CD Walter, *Electronics Letters v 31 no 4 (16/2/95) pp 263–264*

The author shows how to organise hardware for Montgomery multiplication in such a way that almost all the adders are kept busy for almost all the time, regardless of the length of the multiplicand. The trick is in managing the propagation of quotient digits when reductions are performed, and the effect is that one requires only half the adder depth.

041710 'Computing in the Jacobian of a Plane Algebraic Curve'
EJ Volchek, *ANTS 94 pp 221–233*

The authors extend an algorithm of Brill and Noether to perform addition operations in the Jacobian of a plane algebraic curve over an algebraic number field with arbitrary singularities. If M is the larger of the degree and the genus of the curve, then the cost of addition is $O(M^7)$ field operations.

8 Theoretical Cryptology

041801 'Homomorphic threshold schemes, k-arcs and Lenstra's constant'
S Barwick, Y Desmedt, P Wild, *Cirencester 93 pp 95–102*

Homomorphic threshold schemes have the property that if shares a_i can be used to reconstruct the secret A and b_i to reconstruct B, then $a_i \circ b_i$ can reconstruct $A \circ B$. previous schemes, defined over an arbitrary finite Abelian group, had the restriction that the number of shares was limited by the smallest prime factor of the group order. The authors show that this restriction can be overcome by considering the group as a module over some suitable extension of the integers.

041802 'Graph Decompositions and Secret Sharing Schemes'
C Blundo, A De Santis, DR Stinson, U Vaccaro, *Journal of Cryptology v 8 no 1 (1995) pp 39–64*

The authors survey the information rate of the graph of a secret sharing scheme. They look at upper bounds based on entropy arguments, and lower bounds from graph decompositions; the latter case involves linear programming. Some general results are proved on the information rate of paths, cycles and trees, and specific results are given for the 30 connected graphs on five vertices or less.

041803 'A Perfect Threshold Secret Sharing Scheme to Identify Cheaters'
M Carpentieri, *Designs, Codes and Cryptography v 5 no 3 (May 95) pp 183–187*

The author discusses the evolution os secret sharing schemes which detect attempts to cheat, and presents a perfect and unconditionally secure (k, n) threshold scheme each of whose participants' secret amounts to $k + 2(n - 1)$ elements of a finite field rather than the previous $n + 2k - 3$.

041804 'Disenrollment capability of conditionally secure sharing schemes'
C Charnes, J Pieprzyk, *ISITA 94 pp 225–227*

The paper gives the construction of a secret sharing scheme, using a modification of Shamir's scheme, whose security relies on the difficulty of the discrete logarithm problem. Shareholders use their 'initial conditions' to recalculate new shares if the exiting ones are invalidated.

041805 'Zero-Knowledge Proofs of Computational Power in the Shared String Model'
A De Santis, T Okamoto, G Persiano, *Asiacrypt 94 pp 160–170*

The authors formalise the concept of non-interactive zero knowledge proofs of computational power, and give some implementations for certain types of dense random self-reducible and uniformly generatable problems.

041806 'Multiplicative non-abelian sharing schemes and their application to threshold cryptography'
Y Desmedt, G de Crescenzo, M Burmester, *Asiacrypt 94 pp 2–13*

The authors show multiplicative secret sharing schemes which can be used with threshold signatures which are based on non-Abelian groups to produce perfect zero-knowledge threshold proofs of knowledge.

041807 'Comment - multistage secret sharing based on one-way function'
L Harn, *Electronics Letters v 31 no 4 (16/2/95) p 262*

The author shows a slight improvement in a scheme of He and Dawson (below).

041808 'Multisecret sharing scheme based on one-way functions'
J He, E Dawson, *Electronics Letters v 31 no 2 (19/1/95) pp 93–95*

Multistage secret sharing schemes can be used to reconstruct a number of secrets in order given just one share per participant. The authors show how to generalise this so that secrets can be reconstructed in any order.

041809 'On Sharing Many Secrets'
WA Jackson, KM Martin, CM O'Keefe, *Asiacrypt 94 pp 26–37*

This paper considers unconditionally secure schemes which allow the sharing of more than one secret. Firstly, the authors classify the various access structures which may be combined in such a scheme, develop a connection with matroid theory, and exhibit efficient constructions. Secondly, they extend these results to schemes in which secrets can be used more than once.

041810 'Combinatorial Interpretation os Secret Sharing Schemes'
K Kurosawa, K Okada, *Asiacrypt 94 pp 38–48*

The authors provide a new proof of the lower bound on the size of shares in secret sharing schemes, which is based on combinatorial rather than information theoretic arguments.

041811 'Security of the Center in Key Distribution Schemes'
K Kurosawa, K Okada, K Sakano, *Asiacrypt 94 pp 277–287*

The authors show how to construct key distribution schemes with multiple centres so that even of N centres and M users collaborate, they can gain no information on other users' keys.

041812 'Secret sharing model: GS^3'
PL Lin, JG Dunham, *Electronics Letters v 30 no 25 (8/12/94) pp 2116–2118*

The authors define an (l, p, r, n) secret sharing scheme to be such that l shares out of n reconstruct, p or fewer shares yield no information, and r or fewer cheaters cannot affect the reconstruction of the secret. They calculate some information theoretic bounds on such schemes.

041813 'Some applications of coding theory to cryptography'
JL Massey, *Cirencester 93 pp 33–47*

The author surveys the applications of coding theory in cryptography, including the construction of secret sharing schemes and resilient functions. Dual codes give a useful additional insight: a q-ary code whose dual has minimum distance t yields a perfect local randomiser of order t, a k-resilient function for k at most t, and a simple (k, n, q) orthogonal array for k at most $t - 1$. A new approach to defining the nonlinearity of a Boolean function is also suggested.

041814 'Incidence Structure for Key Sharing'
T Matsumoto, *Asiacrypt 94 pp 288–297*

The author investigates schemes in which any two entities will share a common key. These can be characterised in terms of incidence structures, and can be used to store secrets in multiple tamper-resistant modules.

041815 'The role of information theory in cryptography'
UM Maurer, *Cirencester 93 pp 49–71*

The author reviews the standard information theoretic results on perfect secrecy, authentication and secret sharing. He also shows how Shannon's bounds on the key size required for perfect secrecy can be overcome given a public randomiser, provided one can assume that the opponent has finite memory. Finally, he discusses the wiretap channel and the information reconciliation techniques used in quantum cryptography.

041816 'Lower Bound on the Size of Shares of Nonperfect Secret Sharing Schemes'
K Okada, K Kurosawa, *Asiacrypt 94 pp 14–25*

The authors produce a general lower bound on the size of shares in secret sharing schemes which includes previous results on perfect and nonperfect schemes as special cases.

041817 'How to Simultaneously Exchange Secrets by General Assumptions'
T Okamoto, K Ohta, *Fairfax 94 pp 184–192*

Existing secret exchange schemes assume either a specific number theoretic primitive or a uniformly secure bit commitment function. The authors show that these assumptions can be weakened to the existence of one-way functions and one-way permutations.

041818 'Robust Sharing of Secrets when the Dealer is Honest or Cheating'
T Rabin, *Journal of the ACM v 41 no 6 (Nov 94) pp 1089–1109*

When broadcasting is permitted, the Ben-Or bound on verifiable secret sharing (that up to $(n-1)/3$ players can be dishonest) is cut to $(n-1)/2$. A new tool called information checking is introduced, as is a new, weaker, form of secret sharing in which a dishonest dealer can prevent the reconstruction of the secret.

041819 'Combinatorial Structure of A-codes with r-fold Security'
R Safavi-Naini, L Tombak, *Asiacrypt 94 pp 172–184*

The authors study A-codes that provide r-fold protection for spoofing of order r. It is shown that codes with secrecy correspond to t-designs, while codes without secrecy correspond to orthogonal arrays. This generalises previous results since restrictions on the minimality of the number of encoding rules and on the uniformity of the source are removed (the latter only in the case with secrecy). The authors derive explicit bounds on the number of encoding rules for $r \leq 2$ based on Delsarte's linear programming bound, and construct A-codes from some error-correcting codes.

041820 'Perfect authenticity and optimal A-codes'
R Safavi-Naini, L Tombak, J Pieprzyk, *ISITA 94 pp 235–238*

This paper introduces the notion of perfect authenticity in the context of unconditionally secure authentication systems, and shows that such systems require many keys; the result is very similar to the key requirement in systems with perfect secrecy. The paper also includes a characterisation theorem for optimal A-codes which are defined as A-codes with best possible protection and satisfying information theoretic bounds.

041821 'Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer'
PW Shor, *ANTS 94 p 289*

The author announces Las Vegas algorithms for discrete logarithm and factoring which run in random polynomial time on a quantum computer.

041822 'Authentication Codes that are r-fold Secure Against Spoofing'
L Tombak, R Safavi-Naini, *Fairfax 94 pp 166–169*

The authors give an improved lower bound on the number of encoding rules for authentication codes that are r-fold secure against spoofing, and characterise the case with a minimum number of encoding rules. This extends Stinson's characterization by removing the condition of uniform source distribution. It is shown that if the rth order statistic of the source is uniform, r-fold security against spoofing follows from perfect protection of order r.

041823 'On the Construction of Authentication and Secrecy Codes'
TV Trung, *Designs, Codes and Cryptography v 5 no 3 (May 95) pp 269–280*

The author presents recursive constructions for A-codes based on t-designs and on Stinson's authentication perpendicular arrays, and gives a table of known codes.

041824 'Coding theorem for the protection of parameter estimation in Shannon cipher system'
H Yamamoto, *JW-ISC 95 pp 61–65*

This paper examines the coding problem for the Shannon cipher system with a compound source.

9 Book Reviews

'CRYPTOLOGY'
Albert Beutelspacher, translated by Chris Fischer
The Mathematical Association of America, 1994; ISBN 0-88385-504-6

This book is one of a series designed to make modern mathematical topics available to the general public. It starts off with historical ciphers such as monoalphabetics and Vigenère, and proceeds from there to the index of coincidence, the unicity distance and Shannon's theory. It then tackles authentication in the form of passwords and zero knowledge proofs, and goes on to give a gentle introduction to RSA and Diffie-Hellman. The last chapter is on anonymous communications.

The level is about that of secondary school, and the book might be a useful addition to school libraries.

'A COURSE IN NUMBER THEORY'
HE Rose (second edition)
Oxford Science Publications, 1994; ISBN 0-19-853479-5

This book is one of the more comprehensive introductions to number theory which we have reviewed: in addition to the basics such as modular arithmetic and Diophantine analysis, and traditional advanced topics such as partitions and the prime number theorem, the author covers character sums, genera, the class group, and the theory of elliptic curves.

Results of interest to cryptographers, such as elliptic curve factorisation, are explained in this new edition of the book. The author also gives a brief introduction to the theory of L-functions for elliptic curves, which underlies Wiles' progress on Fermat's last theorem, and discusses the conjectures of Taniyama-Weil and Burch-Swinnerton-Dyer.

We would recommend this book as a postgraduate text, and as a map of the foothills of modern number theory.

'INFORMATION SECURITY — AN INTEGRATED COLLECTION OF ESSAYS'
Marshall Abrams, Sushil Jajodia and Harold Podell (editors)
IEEE Computer Society Press, 1995; ISBN 0-8186-3662-9

This is a collection of 27 essays, most of them co-authored by the editors, which covers many of the areas of concern to secure systems builders in the defence sector. Cryptology is not well covered, but this is more than made up with a mine of information on multilevel secure systems.

Among the topics covered are the history the US DoD approach to secure systems design; we learn, for example, of the history of the Torjan horse, of early attempts to penetrate Multics, and that the original intent of the Bell-LaPadula *-property was to prevent illicit downgrading. This provides much interesting background to the Orange Book; there is also a lot of more modern material on the various technical problems which arise in the construction of various kinds of multilevel database.

However, for this reviewer, one of the most interesting essays was by Clark Weissman on penetration testing, which draws on many years' experience to give the ten most productive things for an attacker to look for. These are past experience with similar systems, unclear design, 'omniscient' security controls which can be circumvented, implicit sharing due to incomplete interface design, deviations from the policy and protection model, wrong assumptions about initial conditions, system specific anomalies, operational shortcuts, poor development practices and implementation errors. These are discussed with many references, and used to support a flaw hypothesis methodology for systematic penetration testing (i.e., attack).

'E-MAIL SECURITY — HOW TO KEEP YOUR ELECTRONIC MESSAGES PRIVATE'
B Schneier
J Wiley and Sons, ISBN 0-471-05318-X

Bruce Schneier's latest book provides a good basic introduction to email security. He starts off with a discussion of privacy and email; the threat model ranges from personal enemies to governments, and the modus operandi can extend from router attacks to traffic analysis.

This sets the stage for a discussion of security tools and mechanisms, from anonymous remailers to encryption. This is not as technical as in his book 'Applied Cryptography', but aims to give a working knowledge of PEM and PGP. He discusses some of the controversy surrounding the latter product, and describes how to set it up and use it.

The appendices include the PGP documentation, and the RFC's which specify PEM. This book should appeal to all security managers involved in getting their companies on to the Internet, as well as to individuals who want to understand the practicalities of email encryption.

'DATABASE SECURITY'
Silvano Castano, Mariagrazia Fugini, Giancarlo Martella, Pierangela Samarati
Addison-Wesley, 1994; ISBN 0-201-59375-0

This book covers database security, and much more. It starts off with an introduction to database technology, and continues to provide a grounding in modern computer security concepts, from abstract access control models through to the gritty detail of fielded products such as RACF and a number of multilevel Unices.

Having dedicated a little over two hundred pages to this foundation, it goes on to spend the same again on examining the various problems encountered in building secure database systems and to describe a number of experimental solutions. The various mechanisms used in existing multilevel systems — integrity lock, kernelised, replicated and trusted subject architectures — are described first, and experimental multilevel systems such as SeaView are compared with commercially available products.

Next, there are chapters devoted to statistical security techniques and intrusion detection, and finally the last chapter gives an extensive overview of current research directions, including active and object-oriented databases, message filters, ORION and SORION, and models by Bertino-Wiegand and Millen-Lunt. In conclusion, this is a thorough book, and a perfectly suitable introduction for graduate students wishing to do work in the field.

‘THE LAW OF ELECTRONIC COMMERCE: EDI, FAX AND EMAIL’
B Wright
Little, Brown 1991; fourth edition (with supplement) 1994

The author starts with a broad overview of computer security mechanisms and of the law of authentication. For example, lawyers in the nineteenth century resisted typewriters, on the grounds that contracts could easily be altered; and to this day, different jurisdictions have different rules on whether paper documents must be signed on each page or just once.

From this argument follows that, contrary to conventional cryptologic wisdom, commercial law generally does not require that a signature be ”secure” to be legally effective. In fact, the defining feature of a signature is the intent of the signer; a typed name at the bottom of an email is perfectly valid, barring future precedents to the contrary. Of course it can be forged, but then so can the manuscript signatures on which commerce has been based for centuries.

That is good news for e-mail, and electronic commerce in general; however case law has led to a lot of complications in the case of paper documents. There are differing authentication requirements for fraud, for executors, for suretyship, for property deals and for long term contracts. The implied caveat is that a reasonable man should expect that cryptographic evidence will also become a complex business with the passage of time.

Issues of the admissibility of computer evidence are then discussed. It used to be the case that an extensive foundation had to be laid before introducing it; now, however, the courts are becoming more relaxed. Authenticity tends in practice to be founded on the creation procedure, and a claim of custody thereafter; so a trusted third party must be insulated from the incentive and the ability to falsify a record - a point established in the Irangate trials. Interestingly, in the USA (as in Britain) evidence must have been produced in the normal course of business, not specifically for future litigation. The moral here is that traders should implement explicit and rational record control policies.

Many other topics are discussed, such as directors’ liability for contingency planning, national archives, wire fraud, the Computer Fraud and Abuse Act of 1986, and the various EDI contracts recommended by the American Bar Association and others.

This book is like a breath of fresh air after many of the debates on this subject in the technical press and at conferences. Ben Wright is a real practising Dallas lawyer, and he goes over a lot of US law without, as so many law books do, managing to send the reader to sleep.

How to Subscribe

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

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

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

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

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

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

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

Name: ....

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

Cardholder Address: ....

....

....

Delivery address (if different) ....

....

....

Email address: ....

Signature: ....

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