Computer and Communications

Security Reviews

Volume 3 Number 2 (June 1994) ISSN 1352-6278

CONTENTS

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

Editorial

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

Cirencester III: Third Conference on Cryptography and Coding, 16-18/12/91, Cirencester, England; *Proceedings published 1993 by OUP, ISBN 0-19-853691-7*

New Paradigms: New Security Paradigms Workshops, 1992 and 1993, Little Compton, Rhode Island; *Proceedings published by IEEE (1993) ISBN 0-8186-5430-9*; some papers were abstracted from the preproceedings in volume 2 no 3

Scintilla 94: Symposium on Data Security - Use, Misuse and Abuse, 13/1/94, University of Twente, Enschede, Netherlands; *proceedings published by Scintilla*

SCIS 94: 1994 Symposium on Cryptography and Information Security, 27-29/1/94 Lake Biwa, Japan; *proceedings published by the Institute of Electronics, Information and Communication Engineers*; continued from v 3 no 1

ISOC 94: Internet Society Symposium on network and Distributed System Security, 3-4 February 94, San Diego, California; *proceedings published by Internet Society 1994*

ANTS 94: First Algorithmic Number Theory Symposium, Ithaca, New York, 7-9/5/94; *Proceedings to be published in Springer LNCS series*

Eurocrypt 94: 9-11/5/94, Perugia, Italy; *Proceedings to be published in Springer LNCS series*; page numbers given here refer to preproceedings

Oakland 94: 16-18/5/94, Oakland, California; *Proceedings published by IEEE press ISBN 0-8186-5675-1*

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

Statutory Information

'Computer and Communications Security Reviews' is published quarterly by, and is copyright of Northgate Consultants Ltd, whose registered office is:

Northgate Consultants Ltd
Ivy Dene, Lode Fen
Lode, Cambridgeshire,
United Kingdom CB5 9HF

Subscription rates, conditions and ordering details are on the inside back cover.

1 Applications and Engineering

032101 'Barclays winning card fraud war'
D Austin, *Banking Technology (April 94) p 5*

Card fraud suffered by Barclays Bank dropped from £32.3m in 1992 to £22.9m in 1993. £1m of the saving was due to an expert system which identifies suspicious transactions; other factors were delivering cards more securely and authorising more transactions.

032102 'EMI urges curbs on electronic purses'
D Austin, *Banking Technology (June 94) p 10*

The European Monetary Institute has urged governments to stop non-banks issuing electronic money, in order to maintain control over the money supply. This is opposed by some card issuers.

032103 'Swiping card fraud'
D Austin, *Banking Technology (April 94) p 11*

Recent UK banking industry figures show a fall in card fraud from £165m in 1992 to £129.8m in 1993. The higher level of credit card authorisations is believed to be the biggest single factor.

032104 'A network perimeter with secure external access'
FM Avolio, MJ Ranum, *ISOC 94 pp 109 - 119*

The authors describe a firewall designed by TIS and describe its underlying design assumptions and security policies. User authentication is by challenge-response, whether using a crypto token or a one-time password list; email is encrypted using PEM; and secure telnet is also supported.

032105 'Keeping Secrets a Personal Matter with the Exponential Security System'
T Beth, *Cirencester III pp 1 - 10*

This article describes TESS, a security system developed at EISS Karlsruhe. It is based on using modular exponentiation to provide one-way hash functions with homomorphic properties.

032106 'AT&T pushes forward with smart card'
E Brennan, *Cards International no 108 (25/4/94) p III*

AT&T will issue smart badges to its 256,000 US employees in the third quarter of 1994. They will be used for ID, access control, photocopiers, in cafeterias and for employee benefits. Cards are also being supplied to Chemical Bank, with a view to establishing a card for New York city; and the market for campus cards will also be targeted.

032107 'A Block-sorting Lossless Data Compression Algorithm'
M Burrows, DJ Wheeler, *DEC SRC Research Report no 124 (May 1994)*

The authors introduce a new compression technique: blocks of text are sorted to maximise their accessible redundancy, and then more conventional techniques are applied. A number of variants are possible, but the basic algorithm gets compression of 2.43 bits per character on the Calgary Compression Corpus (which is as good as the better statistical coders) while using cpu resources comparable to those needed for much less efficient schemes.

032108 'What You Are ... Not What You Have'
R Carter, *International Security Review Access Control Special Issue (Winter 93/94) pp 14 - 16*

The author surveys biometric recognition technologies and applications, with particular emphasis on fingerprint recognition techniques. He discusses the two main families of recognition algorithms and their drawbacks; a number of people such as manual workers and pipe smokers damage their fingerprints frequently, and both the young and the old have faint prints.

032109 'Cryptographic Degradation of DES in Block and Stream Cipher Modes in a Digital Mobile Communication Link'
JY Chouinard, G Ferland, *SAC 94 pp 159 - 169*

The authors investigate how well the various block encryption modes work with error correction in a mobile radio application. They used the measured radio channel characteristics for Quebec

City, and simulated the channel bit rate for all four DES modes, with BCH coding following encryption. They found that the error correction was not necessarily effective, and that once interleaving effects were taken into account, only output feedback mode was really satisfactory.

032110 'The breadth of Shamir's secret sharing scheme'
E Dawson, D Donovan, *Computers and Security v 13 no 1 (Feb 1994) pp 69 - 78*
The authors review Shamir's secret sharing scheme, and the development of derived schemes which resist cheating by participants or which implement arbitrary access structures. They show how secret sharing with disenrollment can be incorporated into such schemes by prepositioning masked shares of a number of keys.

032111 'Banks claim victory as battle against card fraudsters hots up'
Financial Technology International Bulletin v xi no 9 (May 94) p 3
Between 1992 and 1993, Barclays reported falls in credit card fraud of 29% to £22.9m and in debit card fraud of 27% to £12.1m. In the whole of the UK, fraud on VISA cards fell 13% in the first four months of 1993.

032112 'Banks may be left behind in the chip card race'
Financial Technology International Bulletin v xi no 8 (April 94) p 2
This article describes the Smart Card 94 conference in London. One of the speakers warned that providers of services such as pay-TV, public transport and mobile communications could be at least as influential as the banks in setting standards.

032113 'Self-service banking boom predicted'
Financial Technology International Bulletin v xi no 8 (April 94) p 2
This article describes a number of moves in the booming market for ATMs and related products, such as new product launches, acquisitions and plant openings.

032114 'VISA forms global purse consortium'
Financial Technology International Bulletin v xi no 8 (April 94) pp 1 & 12
This article reports the formation of VISA's smartcard consortium, a reply from the Mondex banks, and some smartcard developments in South Africa.

032115 'Technologies for Multimedia Communications'
JL Flanagan, *Proceedings of the IEEE v 82 no 4 (April 94) pp 590 - 603*
This article surveys the tools available for building multimedia applications, including automatic recognition of speakers, and discusses the various properties of audio, visual and tactile interfaces to a system. These have been integrated in an experimental system (HuMaNet) at At&T Bell Labs; future directions include face recognition and automatic lipreading. This technology is expected to be fielded within a decade, as GFlops processors become common in workstations.

032116 'Self-Nonself Discrimination in a Computer'
S Forrest, AS Perelson, L Allen, R Cherukuri, *Oakland 94 pp 202 - 212*
The authors explore the possibility of basing the detection of viruses and other unauthorised code on the model provided by the immune system. A large number of 'antibodies' are randomly generated, and those which interact with the authorised system are deleted; the survivors form a 'detector set' which is continually matched against the system to detect foreign activity. Empirical results indicate that most of the work is in generating this set, and that thereafter the technique is efficient. It has the advantage that as each of an organisation's systems would have a different detector set, an attack which defeats one of them would not necessarily defeat them all.

032117 'BAfirewall: A Modern Firewall Design'
R Ganesan, *ISOC 94 pp 99 - 108*
The author describes a firewall developed by Bell Atlantic. It is integrated with Kerberos, and supports traffic between protected sites; it has router based filters, with a specification language which allows the degree of filtering to be controlled locally.

032118 'The Smart Option'
Y Girardot, *International Security Review Access Control Special Issue (Winter 93/94) pp 23 - 24*
The author describes the Bull CP8 smartcard, and its use in access control. He discusses some of its security features, such as the fact that it cannot be run at a reduced clock speed.

032119 'The S/KEY one-time password system'
NM Heller, *ISOC 94 pp 151 - 157*
S/KEY is a one-time password system for user authentication; each password is a one-way hash of the following password. It was developed by Bellcore, and is available on the Internet for Unix, DOS and Macintosh machines.

032120 'Inter-LAN security and trusted routers'
P Hoff, P Spilling, T Bjørke, *ISOC 94 pp 79 - 88*
The authors describe an IP-based encryption device which provides trusted router and firewall services. It allows the creation of secure islands in the Internet, and for users in these to link up using and-to-end authentication and encryption; unencrypted traffic can be let through to designated machines such as mail and news servers.

032121 'A New Anonymous Communication Scheme and its Application to Mobile Communication Systems'
S Houmura, R Sakai, M Kasahara, *SCIS 94 paper 11A (in Japanese)*
The authors propose and examine a version of Mix-net, in which the choice of message routing is used to hide the location of communicants.

032122 'Fissures and chips'
C Johnstone, *Banking Technology (June 94) pp 32 - 33*
This article describes some of the politicking behind the joint work on smartcard standards by VISA, MasterCard and Europay. The physical and electrical standards have been agreed, but there have been rows over the extent to which offline transactions are to be supported.

032123 'Standards for smartcards'
D Jones, *Banking World (May 94) p 33*
The author reports on a consortium set up by VISA to develop standards for a global electronic purse; the member institutions include France's Cartes Bancaires.

032124 'Security Improves with NetWare 4'
N Kelson, *INFO Security News v 5 no 2 (Mar 94) pp 30 - 33*
This article discusses security enhancements in Novell NetWare, version 4. This has improved administration (ease of setting up and managing users), management reporting (of administrator access to sensitive system configurations) and user authentication (both at logon and afterwards).

032125 'External Consistency in a Networking Environment'
LJ La Padula, JG Williams, *New Paradigms pp 131 - 137*
The authors describe how to work systematically from a description of an enterprise, through trust requirements, to external and internal systems requirements. Existing security models fail to tackle the importance of recognising and correcting errors. These issues are discussed in the context of electronic wallets.

032126 'Spread-Spectrum Technology for Commercial Applications'
DT Magill, FD Natali, GP Edwards, *proceedings of the IEEE v 82 no 4 (April 94) pp 572 - 584*
Spread spectrum techniques are an important antijamming and privacy technique in many applications, and are migrating from the military world to commercial systems such as GPS, cellular telephones and the new ISM (instrumentation, scientific and medical) band. This article provides an overview of techniques and systems.

032127 'Untrustworthy Participants in Perfect Secret Sharing Schemes'
K Martin, *Cirencester III pp 255 - 264*

The author discusses how to cope with revoking members of a secret sharing scheme. He argues that just publishing the affected share could be unsatisfactory, and proposes that enough shadows should be distributed to each participant in advance so that the access structure can be recreated over an open channel if anybody drops out.

032128 'Card fraud down for the first time'
R Martin, *Cards International no 108 (25/4/94) p 2*

UK banks reported overall plastic card fraud of £129.8m in 1993; this was down 21% on 1992. Credit is given to increased authorisation levels, more secure delivery and better education.

032129 'Is VISA serious?'
R Martin, *Cards International no 107 (8/4/94) pp 8 - 9*

The author asks whether VISA's recent smartcard standards initiative is a genuine commitment, or just a defensive ploy. He also touches on Britain's Mondex and other pilot projects.

032130 'Mondex: The way forward?'
R Martin, *Cards International no 104 (24/2/94) p 9*

The recently announced Mondex system has been criticised by the Belgian national payments system for having defective cryptography, in the sense that electronic money may be introduced into the system without the bank knowing anything. In addition, whenever anyone loses his card, the issuing bank pockets from the remaining balance.

032131 'Methods of Quantum Cryptography'
H Matsueda *SCIS 94 paper 15A (in Japanese)*

The author reviews work on quantum cryptography and proposes two additional techniques for further study.

032132 'Who pays the bills?'
E McCullagh, I Ryan, *Cards International no 108 (25/4/94) pp 8 - 11*

This article surveys the banks' position on liability for lost plastic cards, and the resolution of disputed card transactions, in a number of countries. In Italy, the customer is liable until he reports the loss to the police and takes a copy of their report to the bank; in Germany, the customer is in theory liable only for the first 10% or DM100, but in practice the banks try to pass the blame on her, and litigation is in progress; insurance is purchased by the cardholder in France, and the card issuer in Japan; while in Singapore, the bank pays all but the first $100. The EC still has no plan to intervene with a directive.

032133 'Informatiebeveiliging door cryptografie'
H Oostveen, A Rozemeijer, *Scintilla 94 pp 87 - 97 (in Dutch)*

The authors provide an overview of encryption technology and describe a number of products available from DATAD in the Netherlands.

032134 'Visual Cryptography'
M Naor, A Shamir, *Eurocrypt 94 pp 1 - 12*

The authors show that visual information can be protected in such a way that it can be decoded using the human eye rather than by a computer. They hide pictures by splitting them into seemingly random patterns of dots: when these are superimposed, the picture appears. The technique has perfect secrecy (in Shannon's sense), and can be used to hide signatures on ID cards so that they are only legible through a special filter. It can also be generalised to a k out of n secret sharing scheme (for small k and n).

032135 'Personal paranoia'
J Newman, *Banking Technology (May 94) pp 30 - 32*

Banks have problems with data protection - customers object to the use of personal information for marketing purposes, and there has been bad publicity about journalists and private detectives getting hold of account information from staff. The EC is trying to tighten up data protection laws, as these vary widely across Europe, from good in Germany to nonexistent in Greece; but the banks are fighting this on the grounds that it could be expensive.

032136 'Simple Encryption via XOR'
MR Parker, *PC Techniques v 5 no 2 (Jun 94) pp 35 - 38*
This article presents and discusses a variant of the Vigenère cipher in PASCAL.

032137 'Smile, you're on camera'
M Reynolds, *The Banker (March 94) pp 76 - 77*
The author describes a current ATM court case in the UK and a number of ATM fraud techniques. One response from the banks has been the use of cameras, with the Bank of Scotland and Barclays having used these since July 92 and August 93 respectively.

032138 'Estimating population from repetitions in accumulated random samples'
T Ritter, *Cryptologia v XVIII no 2 (April 1994) pp 155 - 190*
The author considers the problem of estimating the real diversity of a random number generator by counting the number of values found two or more times in a sample of outputs. He deals with values sampled more than twice by transforming them to an 'equivalent' number of doubles, and, on the assumption of a Poisson distribution, shows how to predict the population size. His analysis is supported by empirical simulations.

032139 'Card fraud plummets in France'
M Rowe, *Banking Technology (May 94) p 10*
Card fraud was down 45% in France from Ffr 375, in 1992 to Ffr 207m in 1993, according to Cartes Bancaires, despite a 7.6% increase in transaction volumes. Smartcards are credited with a significant rôle in this; and the 1993 rate represents 0.04% of value, against 0.15% on international transactions processed by VISA and MasterCard.

032140 'Nations unite for EDI laws'
M Rowe, *Banking Technology (April 94) p 11*
A number of bodies are involved in EDI standards: the Vienna-based Uncitral is considering making the sender of an authenticated message liable, even if the message was not authorised, and hopes thereby to limit the potential liability of intermediaries such as banks and network suppliers. Negotiable instruments such as bills of exchange are also being studied, and the EC is involved through its 'TEDIS' programme.

032141 'Audit-by-receiver paradigms for verification of authorisation at source of electronic documents'
S Russell, *Computers and Security v 13 no 1 (Feb 1994) pp 59 - 67*
The author considers how a receiver is to know that an electronic document is authorised (ie, signed by the right combination of people). In Fischer's model, the organisation's certificate contains this information; it is proposed that this could be simplified by revealing the underlying rules. This would simplify certificates, though it might reveal more about the organisation's internal structure.

032142 'Privacy Enhanced Mail Modules for ELM'
S Russell, P Craig, *ISOC 94 pp 21 - 34*
The authors describe an enhancement of the ELM mailer to include DES encryption. Initial master keys are manually distributed, and there are modules to provide both privacy and manipulation detection.

032143 'Security Issues with Enterprise Multimedia'
M Shain, *Computers and Security v 13 no 1 (Feb 1994) pp 15 - 22*
This article discusses a number of countries' practices in economic espionage, and reviews the techniques commonly used for both overt and covert collection of information. The move

from paper documents and physical meetings to multimedia systems will increase the exposure of companies which use it.

032144 'The X.509 Extended File System'
RK Smart, *ISOC 94 pp 129 - 137*

The author describes a distributed file system for X.509 certificates. It has a number of security mechanisms to assure a user of a file's integrity; these work by a series of endorsements which allow a number of authorities to sign the file.

032145 'Managing the Transition to OSF DCE Security'
S Tikku, S Vinter, S Bertrand, *DCE - The OSF Distributed Computing Environment (Springer LNCS v 731) pp 147 - 161*

The authors describe a set of tools, provided with Siemens Nixdorf's DCE and SINIX, which enable the access control mechanisms of DCE and Unix to interoperate safely. The product's final goal is unified administration under DCE.

032146 'Security in telecommunication applications in Europe'
HJWM van de Pavert, *Scintilla 94 pp 28 - 35*

The author gives an overview of telecommunications security, with particular reference to the use of smartcards as the Subscriber Identity Modules which control access to the GSM mobile telephone network.

032147 'Scam-busters"
A Warner, *The Banker (May 94) pp 68 - 70*

This article discusses frauds involving high value instruments such as standby letters of credit and prime bank guarantees. A number of firms offer technical services such as systems security consultancy and investigations, while the villains include money launderers and organised groups who target bank employees. At the other end of the scale, non-plastic fraud against UK retail customers (such as forgery and counterfeiting) actually fell 26% to £20m in 1993.

032148 'Trusted to untrusted network connectivity'
WJ Wied, *ISOC 94 pp 89 - 98*

The author describes a firewall, 'MANIAC', developed by Motorola to control Internet access and to provide address translation for private networks. Its 'double firewall architecture' has one machine in each of the trusted and untrusted domains, and they are connected via a screening router. Bridges are provided for ftp and telnet.

032149 'Identity Verification using Weighted Personal Characteristics'
Y Yamazaki, N Komatsu, M Tsuchiya, *SCIS 94 paper 5C (in Japanese)*

The authors study whether characteristics of a person's handwriting may be used to authenticate that person. They have used a neural net to distinguish persons successfully according to the angles between written strokes.

2 Operating System and Database Security

032201 'Collecting Garbage in Multilevel Secure Object Stores'
E Bertino, LV Mancini, S Jajodia, *Oakland 94 pp 106 - 120*

If a garbage collector preserved a low object that was only referred to by a high one, this would create a covert channel; the authors propose to upgrade such dangling objects, and provide a mechanism to do this with an untrusted copying collector: each level has its own collector, and there is a trusted collector monitor which activates them in sequence from low to high.

032202 'Mode Security: An Infrastructure for Covert Channel Suppression'
R Browne, *Oakland 94 pp 39 - 55*

A system that does not share resources dynamically between different security levels is secure, but may be ineffective; if it does share them, it risks being full of covert channels. The author proposes, as a happy medium, that a system should have a number of modes, in each of which a fixed proportion of resources are allocated to each level. By quantifying how and how often mode switches occur, the author is able to quantify the maximal damage down by the residual covert channels that arise during these mode changes. The paper concludes by discussing the idea of mode security in a practical light.

032203 'A Mathematical Framework to Implement Statistical Databases'
M Costa, *ACM SIGSAC v 12 no 2 (April 1994) pp 6 - 12*

The author discusses the use of matrix algebra to tackle inference control problems in statistical databases, and shows how to implement simple schemes in SAS/IML.

032204 'Computer Security by Redefining What a Computer Is'
Y Desmedt, *New Paradigms pp 160 - 166*

The author argues that falling hardware costs make it foolish to use multiuser systems in sensitive applications. He discusses the nature of a world in which everyone has a personal computer, with a smartcard to hold crypto keys, and all larger scale processing is based on authenticated transactions.

032205 'Logische toegangsbeveiliging: voorwarde voor gegevensbescherming'
JGP Frints, TB Vreeburg, *Scintilla 94 pp 36 - 41 (in Dutch)*

The authors describe a security model used by a Dutch accounting firm to track logical access paths through systems and applications software.

032206 'The Complexity and Composability of Secure Interoperation'
L Gong, XL Qian, *Oakland 94 pp 190 - 200*

The authors propose two principles of secure interoperation: autonomy (that legal local access stays legal) and security (that forbidden local access stays forbidden). The question then becomes how many crossdomain access links can be granted without breaking local security. In general this problem is NP-complete, but if the access structures are totally ordered, the problem can be solved in polynomial time; and interoperation can be imposed on any structure whose graph is acyclic.

032207 'Security is Fuzzy'
HH Hosmer, *New Paradigms pp 178 - 184*

The author discusses how fuzzy logic might be applied to computer security to deal systematically with vague concepts such as 'grave risk' and 'small covert channel bandwidth'. She argues that it might be particularly good at dealing with the problems of multipolicy environments.

032208 'The Multipolicy Paradigm for Trusted Systems'
HH Hosmer, *New Paradigms pp 19 - 32*

Many real world systems have multiple security goals, which are not always consistent; a number of examples are given from both military and civil government applications. Policy conflict resolution is important, and the author develops a multipolicy paradigm in which metapolicies are used to clarify the importance, the assumptions and the scope of individual policies in some given context. A number of possible implementation strategies are discussed.

032209 'Information System Security Engineering: A Spiral Approach to Revolution'
DM Howe, *New Paradigms pp 53 - 56*

NSA is now using Boehm's spiral model to tackle security engineering problems; prototypes are used to drive both theory and practice in an incremental way. This is perceived as being much less risky than revolutionary change; it is being used to extend the traditional models to denial of service attacks and to consider the problems of hostile code more thoroughly. Work has also been done by the Military Airlift Command on an MLS testbed using these ideas. The Canadian CTPEC turns out to be more suited to the spiral model than TCSEC.

032210 'Ensuring Security in Interrelated Tabular Data'
R Kumar, *Oakland 94 pp 96 - 105*

Agencies publishing tabular data often have to suppress confidential items, and it is important to know how many other items also have to be suppressed in order to prevent an attacker working back from row and column totals to derive or estimate the missing data. Deciding which cells need to be suppressed is NP-hard, but the author shows how it can be broken down and tackled by linear programming techniques. The basic idea is to treat secondary suppressions in one table as primary suppressions in the next.

032211 'Concurrent Automata, Database Computers, and Security: A "New" Security Paradigm for Secure Parallel Processing'
TY Lin, *New Paradigms pp 94 - 104*

The author considers the security of database computers, and in particular the effects of clustering. He advances a Petri net model which can safely replace logical with temporal clustering.

032212 'Isolation-only transactions for mobile computing'
Q Lu, M Satyanaranyanan, *ACM Operating System Review v 28 no 2 (April 1994) pp 81 - 87*

Read-write conflicts become a much more serious threat to integrity with mobile clients, because of intermittent connectivity. The authors report a system, Coda, which gives clients their own disk caches and provides an isolation transaction which will accept serialisable updates.

032213 'New Paradigms for High Assurance Software'
J McLean, *New Paradigms pp 42 - 47*

Current security models focus on the confidentiality of wholly deterministic systems; they ignore integrity, availability and noise. One consequence is that high-bandwidth covert channels are often not discovered until after systems have been coded, at which point they are expensive to eliminate. There are other shortcomings to the TCSEC approach, among which is the fact that vast amounts are spent on protection without much idea of what benefit has actually been bought; so more work is needed on the economics of actual attacks.

032214 'Implementation of a Secure File Transfer System'
K Nakagawa, K Sakurai, T Okamoto, *SCIS 94 paper 1D (in Japanese)*

This paper describes an implementation of a secure networked filing system using a key distribution protocol based upon the RSA public-key cryptosystem and a symmetric session key. The authors contrast the security of their scheme with Kerberos and give performance figures.

032215 'A Note on a UNIX Based Access Control System to Avoid Indirect Information Leakage'
S Ozaki, T Matsumoto, H Imai, *SCIS 94 paper 6A (in Japanese)*

The standard UNIX file access permissions are chosen by the owner of a file (usually the person who first opened it for writing). If a file is opened for reading its contents may be copied, either deliberately or inadvertently, to a file with less strict access permission - in other words any user with read permission to a file may downgrade its security. The authors propose a scheme by which a hierarchical security model, such as that proposed by Bell and La Padula, might be imposed on a UNIX filesystem.

032216 'Inference Channel-Free Integrity Constraints in Multilevel Relational Databases'
A Qian, *Oakland 94 pp 158 - 167*

This paper takes a logical approach to studying integrity and inference in multilevel relational databases. The paper includes several logical constraints for dealing with inference channels.

032217 'A Secure Group Membership Protocol'
MK Reiter, *Oakland 94 pp 176 - 189*

In a distributed system, there may be a disagreement about what processes are operational, especially if they are continually starting and stopping; group membership protocols achieve a consistent view. The paper proposes a protocol which resists corruption of up to one third of the members, and can remove corrupt members once exposed; adding members takes the agreement of one third, and removing takes two thirds, of the current membership. The protocol is based on signed point-to-point messages, and a manager process; the members either agree to his suggestions or throw him out, and in the latter case the highest ranked process trusted by at least a third of the members takes over.

032218 'Application Level Security Using an Object-Oriented Graphical User Interface'
T Rooker, *New Paradigms pp 105 - 108*

TCSEC was developed for mainframe operating systems; it is hard to apply to modern workstations because of the many layers of software. In this environment, it makes sense to provide security at more than one layer, and the application layer is particularly important. Simplifying the development of secure applications is the most important challenge facing researchers.

032219 'The Reference Monitor: An Idea Whose Time Has Come'
T Rooker, *New Paradigms pp 192 - 197*

Now that operating systems tend to be built on modular lines with small kernels, the reference monitor concept may be much easier to implement, and give much more assurance, than when it was first mooted twenty years ago. This is discussed with specific reference to Windows NT, Mach and the GNU Hurd architecture.

032220 'Identification and Authentication when Users have Multiple Accounts'
WR Shockley, *New Paradigms pp 185 - 191*

Letting users have multiple accounts can endanger a number of policies such as Clark-Wilson, and military policies which deny access by certain named users. The author argues for the use of biometric technology, together with cryptographically sealed account records to provide whatever anonymity or privacy is called for.

032221 'Security In An Object-Oriented Database'
JM Slack, *New Paradigms pp 155 - 159*

The author shows that both secrecy and integrity properties may be implemented in object-oriented systems by limiting the types of messages which an object in a given group can send and receive. In particular, Clark-Wilson and mandatory access control policies can be realised.

032222 'The No-Policy Paradigm: Towards a Policy-Free Protocol Supporting a Secure X Window System'
M Smith, *New Paradigms pp 109 - 117*

Existing access control extensions to X Windows are not interoperable, so the author proposes a protocol for securing X applications which can support a number of different security policies, and discusses the mechanisms involved. His goal is to achieve an industry consensus on these.

032223 'Elimination of Inference Channels by Optimal Upgrading'
ME Stickel, *Oakland 94 pp 168 - 174*

A user is cleared to know A_1, A_2, ... , A_m, but not cleared to know B. However, if B can be inferred from A_1, A_2, ... , A_m, there exists an inference channel. To close it, one could upgrade some of the A_i, but this can be hard in practice. Therefore, one wishes to upgrade the A_i's in a minimum cost way. This paper shows how the Davis-Putman theorem proving procedure can be used, provided that the security lattice is totally ordered; contrasts this approach with those of Su-Ozsoyoğlu and Millen; and finally discusses its implementation on SRI's DISSECT system.

032224 'Modelling and Verification of Covert Channels using Time Petri Nets'
M Tetsuya, T Shigeo, *SCIS 94 paper 6D (in Japanese)*

If an access control matrix has values that change over time, then these changes may be used to implement a covert channel. The authors use Time Petri Nets to discover and model these.

032225 'Extension of Information Security Systems with an AI Approach - Verification of Unsecure Paths in Access Matrices'
M Tetsuya, S Hisao, U Keisuke, S Tsujii, *SCIS 94 paper (in Japanese)*

The authors apply Hayes-Roth's Blackboard Architecture to the discovery of covert channels in multi-level secure databases.

032226 'Towards a task-based paradigm for flexible and adaptable access control in distributed applications'
RK Thomas, RS Sandhu, *New Paradigms pp 138 - 142*

The authors show how security models can be based on tasks rather than on subjects and objects. They provide an example of how this would cope with dual control in a cheque processing application: partially approved vouchers become transient objects.

032227 'Secure Computing with the Actor Paradigm'
B Thuraisingham, *New Paradigms pp 76 - 81*

The author discusses the security aspects of Agha's model of concurrent computation. Providing a multilevel secure version of this involves adding security labels to quite a lot of entities, including tags, communications and addresses.

032228 'Modelling Multidomain Security'
JDJ Vázquez-Gómez, *New Paradigms pp 167 - 174*

The author proposes a model for multidomain security in which all interdomain interactions are controlled in a mandatory fashion, and no attribute translation is permitted. He argues that these controls could be derived from an ordering of the security policies of the constituent domains.

032229 'Extending the Schematic Protection Model - 1: Conditional Tickets and Authentication'
V Varadharajan, C Calvelli, *Oakland 94 pp 213 - 226*

The authors present an extension of Sandhu's Schematic Protection Model, which deals with access privileges and protection structures, so that it can cope with conditional tickets. Conditions may include performing an authentication procedure (which adds an implicit revocation capability), and an algorithm is provided to search the relevant graph and provide a safety proof. The work has been applied to a healthcare system.

032230 'A Shift in Security modeling Paradigms'
JG Williams, *New Paradigms pp 57 - 61*

The author discusses what the trusted computing base would look like if integrity, rather than confidentiality, were the main objective. Systems could be constructed which would warrant some of their outputs as correct, provided that their inputs had been, by accounting for all the possible effects of detected errors. This might be done by keeping a pedigree of all events on which a warranted input depends.

032231 'Neighbourhood Data and Database Security'
K Yazdanian, F Cuppens, *New Paradigms pp 150 - 154*

There may be semantic and other relationships between entries in different databases, which can give rise not just to inference problems but to covert channels as well. The authors suggest that deducibility properties might be used to identify which data items may be dangerously related.

3 Security Management and Policy

032301 'Managing Complexity in Secure Networks'
D Bailey, *New Paradigms pp 2 - 6*

Traditional security policies assume that processors are islands, and that all information flows between them can be comprehended and managed by a single person. This is becoming steadily less realistic, and two new models are proposed. The 'secure telephone' model uses encryption to restrict particular messages to designated counterparties, but in a decentralised way; and the 'VIP protection' model assumes that the environment, although generally benign, will have some very hostile elements, and has particular assets surrounded by guards which screen local traffic.

032302 'The New Software Copyright Law'
A Bundy, H MacQueen, *The Computer Journal v 37 no 2 (1994) pp 79 - 82*

The authors discuss the content and effect of the Copyright (Computer Program) Regulations 1992, which were introduced following the EC directive on the topic and came into force at the beginning of 1993. The regulations allow users to make backups, decompile programs and correct errors, but leave some other issues open.

032303 'Letter to the Editor'
R Courtney, *Computers and Security v 13 no 1 (Feb 1994) pp 34 - 36*

The author deplores the frequent calls for senior corporate management to take more interest in computer security. He argues that security, like other housekeeping tasks, can be delegated in any well run company, and that there may indeed be legal advantages in not informing the board in detail of all the possible threats.

032304 'A New Paradigm for Trusted Systems'
DE Denning, *New Paradigms pp 36 - 41*

Standards of trust change over time: ten years ago, no-one worried about whether a diskette might contain a virus. Trust assessments are based on personal experience, recommendations from friends, or from commercial services such as consumer organisations; ultimately, there is a market in reputation. Thus, ultimately, computer security assessments should be based on customer satisfaction, rather than on assessments of their internal mechanisms. However, TCSEC approach is not just focussed on internals, but also highly risk averse; it therefore stifles innovation, which is required for the success of a market system.

032305 'Yardley's diplomatic secrets'
R Denniston, *Cryptologia v XVIII no 2 (April 1994) pp 81 - 127*

This is a biography of Herbert Yardley, author of 'The American Black Chamber', based on a thesis by Alastair Denniston's son. It also examines an unpublished book by Yardley called 'Japanese Diplomatic Secrets'.

032306 'Managing Network Security'
C Dixon, *Information Security Monitor v 9 no 5 (April 94) pp 5 - 6*

The author provides a management checklist for network security, including the conduct of business impact reviews, annual reviews, and the reviews needed whenever major changes are carried out.

032307 'Encryption ABCs'
RJ Duncan, *INFO Security News v 5 no 2 (Mar 94) pp 36 - 37*

This article presents a concise overview of encryption technology and applications.

032308 'Strategic Briefing - Security'
S Gold, S Mansfield, *Personal Systems in Business (Summer 1994) pp 26 - 38*

Theft of personal computers is increasing rapidly in Britain, and this makes a security policy which includes reliable backup important. The security features of DOS, OS/2 and the LogicLock features of the PS/2 are discussed, as are physical security, anti-virus measures and choosing strong passwords.

032309 'Confidentiality, Integrity, Assured Service: Tying Security All Together'
GL Hammonds, *New Paradigms pp 48 - 52*

The author argues that confidentiality, integrity and availability can all be integrated into a single security model.

032310 'A Clipper Primer'
HJ Highland, *Computer Fraud and Security Bulletin (May 94) pp 13 - 18*

This article covers key escrow; it describes the architecture of Clipper and Capstone, and the controversy which they have engendered. The author prophesies that 'within 90 days (of the chip's release), people will discover how to pass traffic with an invalid or no (LEAF)'.

032311 'Disaster recovery plans: two case studies'
S Hinde, *Computer Audit Update (April 94) pp 6 - 15*

This is a list of the headings under which an unnamed organisation's disaster recover plans were organised.

032312 'Achieving Consistent Security Controls Throughout a Multinational Organisation
N Hoppé, *Computers and Security v 13 no 1 (Feb 1994) pp 23 - 29*

The motivation for security programmes may come from external auditors as well as from internal practitioners, but in order to be effective, security must be promoted at a number of levels at once in a large organisation.

032313 'Computer Systems Security in Slovenia'
A Hufoklin, B Šmitek, *Computers and Security v 13 no 1 (Feb 1994) pp 30 - 33*

The authors report a survey of a number of Slovenian enterprises. 38.7% of them have a computer security function, but in 69.4% of cases a single person carries this responsibility. Only about half the respondents had a security policy, and 11% had been victims of abuse (compared with 72% and 22% in the UK).

032314 'Cryptografie en Beveiliging'
CJA Jansen, *Scintilla 94 pp 6 - 12 (in Dutch)*

The author gives an introduction to cryptography, covering its main uses, the main types of algorithms available, and the management issues.

032315 'Computer Misuse Act - Success or Failure?'
MR Jones, *Information Security Monitor v 9 no 4 (March 94) pp 5 - 7*

The author (an official at Britain's Department of Trade and Industry) describes the origins and main provisions of the Computer Misuse Act, and discusses four cases brought under it. He concludes that no legislative changes are required.

032316 'From the archives - a real fake message'
D Kahn, *Cryptologia v XVIII no 2 (April 1994) pp 150 - 152*

The author discusses a 1916 message from the German embassy in Madrid which proposes to sell the French an obsolete code book through an agent provocateur, and thus feed them false information. This is apparently the only documented case of a spoof on this kind of traffic.

032317 'Distributed and Secure'
R Kay, *Byte Magazine (June 1994) pp 165 - 178*

This article starts off with a survey of access control in heterogeneous networks, discusses a number of access tokens from password generators to smartdiskettes, and goes on to examine Kerberos. There are a number of problems in adapting applications to use this, but Carnegie Mellon's AFS integrates it into the operating system.

032318 'Auditing in distributed systems'
SW Luan, R Weisz, *ISOC 94 pp 139 - 147*

The authors describe the audit features of OSF DCE 1.1. An audit daemon on each machine uses secure RPC to get instructions from an event selector and report events to an audit log.

032319 'Clinton administration report on human rights ignores data privacy issues'
W Madsen, *Computer Fraud and Security Bulletin (May 94) pp 10 - 13*

The author criticises the US State Department's annual report for 1993 on the state of human rights worldwide for ignoring many problems with data privacy. These included systematic wire-tapping scandals in El Salvador, France and Thailand, and other problems in countries as diverse as Germany, Russia, Ireland and Singapore.

032320 'Clinton Approves Clipper, Fails to relax Export Controls'
W Madsen, *Computer Fraud and Security Bulletin (April 94) pp 7 - 9*

The author reports the US administration's approval of key escrow after nine months' consultation, despite opposition from a number of quarters. These include Canada's Communications Security Establishment, which is worried about US snooping on Canadian traffic.

032321 'An Outline of a Taxonomy of Computer Security Research and Development'
C Meadows, *New Paradigms pp 33 - 35*

The author gives a survey of computer security research areas, and highlights some of the topics which are less well understood.

032322 'Status of Information Security Techniques Standardisation in ISO/IEC JTC1/SC27'
K Naemura, T Suga, K Takaragi, S Miyaguchi, *SCIS 94 paper 16C (in Japanese)*

This is a progress report on international standardisation of information security techniques; these include cipher modes, authentication, nonrepudiation, hash functions, evaluation criteria, zero knowledge techniques, and key management. Included is a list of projects dating back as far as 1987.

032323 'Italy and computer crimes (better late than never)'
S Ongetta, *Computer Fraud and Security Bulletin (April 94) pp 16 - 19*

The author describes a new computer crime law introduced in Italy from January 1994. Especially long sentences are available when a security violation is carried out by a public official abusing his powers, by a private investigator, by a systems operator, by means of violence, and against public systems such as those operated by the police, military and health services.

032324 'Avoid Encryption Anarchy'
DB Parker, *INFO Security News v 5 no 3 (May 94) pp 29 - 32*

The author argues that pervasive encryption can lead to abuses: people can lose data if they forget their key, and can even use encryption to hide subversive activities. He proposes that organizations should control encryption strictly, perhaps using some form of key escrow.

032325 'Data-security: regelgeving en beleid in Nederland'
C Prins, *Scintilla 94 pp 14 - 27*

The author gives an overview of legal problems with computer security and cryptography in the Netherlands. The three main problems are the admissibility of digital signatures, free access to information, and law enforcement interests; at present, there is no law allowing a judge to compel access to computer data. There is an extensive bibliography

032326 'The End of Paper Money'
B Schneier, *INFO Security News v 5 no 3 (May 94) p 56*

This article presents a general discussion of the present and possible future uses of digital cash.

032327 'Theoretical Analysis and Simulation of Computer Viruses Prevalence'
Y Sengoku, M Mambo, E Okamoto, *SCIS 94 paper 5A (in Japanese)*

This paper presents a statistical model to predict the spread of computer viruses across a network and suggests requirements to prevent their spread.

032328 'Clipper chip dominates privacy conference'
D Sims, *IEEE Software (May 94) pp 106 - 107*

This report on the recent Fourth Conference on Computers, Freedom and Privacy focusses on the reactions to the Clipper chip and the antagonism displayed between computer professionals and the US government, which was exacerbated by the arrest of an attendee.

032329 'A People Problem'
M Smith, *International Security Review no 83 (Winter 93/94) pp 13 - 19*

The greatest threat to information systems does not come from sophisticated attacks, but from low-tech crime such as theft of media and coercion of employees. The real emphasis should be on using organisation and procedures to provide a defence in depth.

032330 'Pragmatic security in systems development: a European approach'
A Stanley, *Computer Audit Update (March 94) pp 7 - 9*

The author reports a project by the European Security forum to provide guidelines for security during system development. He includes the results of 1990 and 1992 surveys on developers' attitudes, and describes the project methodology.

032331 'How Responsibility Modelling Leads to Security Requirements'
R Strens, J Dobson, *New Paradigms pp 143 - 149*

Responsibility relationships are the key to mapping organisational to technical requirements; they bring out need-to-know policies, audit criteria and a whole lot more. This technique was used to elicit a security model in a healthcare application.

032332 'Policy Considerations for Data Networks'
WH Ware, *Computing Systems Usenix v 7 no 1 (Winter 1994) pp 1 - 44*

The author provides a guided tour of the security problems which beset heterogeneous networks such as the Internet and USA's the forthcoming NII. The public switched network can provide a model; it used to be homogeneous, but has become heterogeneous since the onset of competing carriers. A number of related public policy issues are aired.

032333 'Unix - who manages your system?'
A Webb, *Computer Audit Update (April 94) pp 3 - 6*

The task of managing operating systems was done by experts in the mainframe world, and was neglected altogether by PC users; but now that many firms are introducing distributed systems, they are failing to train staff to manage them. The author reports that over 50% of the Unix systems she sees in audit practice have no designated administrator, and discusses some of the ways in which things go wrong when administration is done my marginally skilled people.

032334 'Business Continuity Planning'
K Wong, *Computer Fraud and Security Bulletin (April 94) pp 10 - 16*

The author presents a number of ideas gleaned from the Bishopsgate bombing and other disasters. These include the value of a clean desk policy, the need to coordinate evacuation plans with neighbours, and the need to bear in mind that the police impose a 400 metre cordon after a bombing, which may be enforced for some time (36 hours in the case of Bishopsgate) - so the main and emergency sites should not be too close.

4 Formal Methods and Protocols

032401 'Prudent Engineering Practice in Cryptographic Protocols'
M Abadi, RM Needham, *Oakland 94 pp 122 - 136*
The authors propose eleven principles to guide designers of cryptographic protocols and help them avoid the more common errors. The underlying reasoning behind these principles is that each message should say what it means explicitly, and that the conditions for it to be acted on should be clear to a reviewer. In particular, the properties of nonces and encryption should be understood, and principals' names, message types and trust relationships should be made clear. For example, encryption can be used to hide data, to bind data or to prevent alteration of data; one must be clear what one is trying to do. Examples are given of how the designers of broken protocols violated these principles.

032402 'X9 Certificate Management'
R Ankney, *ISOC 94 pp 49 - 50*
The author gives a brief introduction to the ANSI X9.30 certificate management standards for wholesale banking. These are based on DEC's DSSA and are designed to minimise the effect of a certification agency's being compromised; revocation certificates distinguish emergencies, and high risk transactions may require two signatures from separate facilities. Certificates contain cosignature requirements and contextual controls such as liability limits, transaction types and time constraints.

032403 'Certified Electronic Mail'
A Bahreman, JD Tygar, *ISOC 94 pp 3 - 19*
The authors present protocols which provide non-repudiation of receipt; two mutually suspicious parties can exchange receipts for email messages. If postmasters are trusted, Alice can send M to Bob's postmaster, who encrypts it, sends it to Bob, gets a receipt and then releases the key; and if no trusted third party exists, the same effect can be achieved using bit commitment and zero knowledge techniques.

032404 'Asynchronous Composition and Required Security Conditions'
N Boulahia-Cuppens, F Cuppens, *Oakland 94 pp 68 - 78*
This paper looks at properties that are preserved under hook-up by extending earlier work of Bieber and Cuppens. The approach taken involves modal logic and concentrates on asynchronous communication. The paper also studies the security problems involved when inputs are blocked and this blocked information is sent back to a subsystem via feedback.

032405 'Generating Formal Cryptographic Protocol Specifications'
U Carlsen, *Oakland 94 pp 137 - 146*
This paper describes the use of CKTS, a modal logic of communications, to analyse cryptographic protocols. Part of the job was creating a system of types for master and session keys, timestamps and so on. Belief evolution is described by formula-based specifications, and one of the advantages is the ability to work back from a protocol description to a formal specification.

032406 'Management of PEM Public Key Certificates Using X.500 Directory Service: Some Problems and Solutions'
TC Cheung, *ISOC 94 pp 35 - 42*
The author examines using a central directory server to interact with local servers and provide PEM certificates and revocation lists for users. This can give rise to denial-of-service attacks, which are affected by the particular cacheing strategy in use. A modified version of TIS/PEM was used to explore these issues, and performance tables are given.

032407 'Public Key Infrastructure Study (PKI)'
S Chokhani, *ISOC 94 pp p 45*
On behalf of NIST, MITRE studied how public keys should be managed for the US government,

and recommended a four layer hierarchy, whose costs would depend on how certificate revocation lists are managed. They also proposed that certification authorities would enjoy extensive immunity from legal liability.

032408 'New Security Paradigms: What Other Concepts Do We Need As Well?'
J Dobson, *New Paradigms pp 7 - 18*

The author surveys those aspects of computer security which have up till now been tackled by formal models and methods. One shortcoming is that, in real life, security policies are complicated by issues of responsibility and authorisation. Thus a proper treatment should include information rights as well as a model, rules and exchange specifications. It should also be driven by the needs of the enterprise rather than by its mechanisms.

032409 'Eliminating Formal Flows in Automated Information Flow Analysis'
ST Eckmann, *Oakland 94 pp 30 - 38*

Automated tools which look for flows of information from High to Low often identify flows that exist formally, but in practice are of a benign nature. This paper looks at the previous work of Fine on this subject dealing with his ft-policy. The major new result is that one can add opaque definitions to Ina Jo to help Ina Flo not point out benign flows. The paper is complete with examples and discussions of the practicality of opaque definitions.

032410 'A Model for Secure Protocols and Their Compositions'
N Heintze, JD Tygar, *Oakland 94 pp 2 - 13*

The authors propose basing protocol analysis on model theory rather than logic. Their model consists of a trace and a belief; traces must be serialisable and beliefs are valid if they can be derived, while a secure protocol is one which preserves valid beliefs. There is a novel approach to freshness: a model is called time-secure if all fresh or shared secrets ultimately expire. It is shown that crypto protocols can be composed securely if (roughly) there are no beliefs involving compound messages or non-principals, and that messages from adversaries do not have a significant effect on the component protocols.

032411 'Specifying and Checking Unix-Security Constraints'
A Heydon, JD Tygar, *Computing Systems Usenix v 7 no 1 (Winter 1994) pp 91 - 112*

The authors describe a system called Miró for specifying and checking security constraints, particularly on file systems. A constraint language is used to express security policies, check that they are realisable, and to verify that an existing configuration is acceptable. The tool is applied to the Grampp-Morris security constraints for Unix.

032412 'A Simple Scheme for Challenge-Response Type Human Identification'
H Ijima, T Matsumoto, *SCIS 94 paper 13C (in Japanese)*

The authors propose an authentication scheme using changing passwords to help resist eavesdropping attacks.

032413 'A complete secure transport service in the Internet'
F Jordan, M Medina, *ISOC 94 pp 67 - 76*

The authors describe a Kerberos extension which supports connectionless and multicast transport protocols. These were developed for the EC's COMANDOS distributed operating system, and the main innovation is a group key distribution service.

032414 'Three Systems for Cryptographic Protocol Analysis'
R Kemmerer, C Meadows, J Millen, *Journal of Cryptology v 7 no 2 (Spring 94) pp 79 - 130*

The three authors describe the use of their respective formal tools (Ina Jo, the NRL Protocol Analyzer and the Interrogator) to search for the flaws in the Tatebayashi-Matsuzakai-Newman protocol. All these systems combine algebraic and state-transition methods, but implement them in different ways; it turned out that Ina Jo uncovered one flaw, while the other two found the other flaw. As a result of the exercise, both the NRL Protocol Analyzer and the Interrogator are having their algebraic capabilities upgraded.

032415 'Applicability of Smart Cards to Network User Authentication'
M Krajewski, JC Chipchak, DA Chodorow, JT Trostle, *Computing Systems Usenix v 7 no 1 (Winter 1994) pp 75 - 89*

The authors discuss the vulnerabilities of Kerberos and report a project to enhance it using smartcards. Here, the card does the crypto processing at the client and thus guards against various Trojan horse attacks on session keys. The experience is described, and requirements for a production smart card enhancement are discussed.

032416 'A Rule-Set Approach to Formal Modeling of a Trusted Computer System'
LJ LaPadula, *Computing Systems Usenix v 7 no 1 (Winter 1994) pp 113 - 167*

The author presents a way to construct formal security models by accumulating rules, and shows how this approach can cope with Unix System V/MLS and Clark-Wilson (inter alia). The basic idea is to make formal modelling more flexible, in that rules can be added to an existing model without a complete rework. Its application to Unix systems is described in some detail.

032417 'Prospect on Security Paradigms'
LJ LaPadula, *New Paradigms pp 62 - 68*

The author tabulates the modeling techniques used in a number of different systems, and how these evolved over time. He shows that the scope of modeling has widened somewhat over the years.

032418 'Bell and LaPadula Axioms: A "New" Paradigm for an "Old" Model'
TY Lin, *New Paradigms pp 82 - 93*

The author presents an axiomatised version of the Bell-LaPadula model. Its main difference is that trusted subjects are replaced by filters; however, this does not eliminate the potential for errors while information is downgraded.

032419 'Security of Numerical Passwords'
H Makino, K Mimori, I Tokuhiro, *SCIS 94 paper 5B (in Japanese)*

Short passwords, such as PINs, are vulnerable to eavesdropping attacks. The authors examine authentication protocols in which a function of the password rather than the password itself is sent across a network, and show that such protocols can often be vulnerable to eavesdropping too.

032420 'Classification of Cryptographic Techniques in Authentication Protocols'
WB Mao, C Boyd, *SAC 94 pp 95 - 104*

Confusion about the purposes of encryption is a common problem for protocol designers, and as the formalisation step usually overlooks whether the object is to conceal or to bind data, cut-and-paste attacks on modes such as CBC can be overlooked. In addition, putting the participants' names into the encrypted part of key setup messages may expose key encrypting keys to the same risks as data encrypting keys. The authors therefore propose that protocol logics should use different notation for encryption depending on whether it is for confidentiality or integrity, even when a symmetric algorithm is being used.

032421 'A General Theory of Composition for Trace Sets Closed Under Selective Interleaving Functions'
J McLean, *Oakland 94 pp 79 - 93*

This paper develops a general theory of composition for noninterference-like security properties. Previous work had considered whether a property is preserved when composed via general hook-up with itself; this research looks at what properties will be satisfied by a system in which components satisfying different properties are composed via various types of composition constructs, and does not even assume that systems are input total. The paper introduces a trace constructor called selective interleaving, and shows how the composition of two channels of zero capacity can create a channel with positive capacity. These channels are similar to the ones McCullough uses to show that noninterference is not composable.

032422 'Integration of Formal and Heuristic Reasoning as a Basis for Testing and Debugging Computer Security Policy'
JB Michael, EH Sibley, *New Paradigms pp 69 - 75*

Security policies can have bugs just as protocols and implementations can, and these can be just as dangerous. However, debugging policies cannot be done by formal techniques alone; it needs heuristic reasoning as well.

032423 'Remote Kerberos authentication for distributed file systems as applied to DCE DFS to NFS file system translator'
T Mistretta, W Sommerfeld, *ISOC 94 pp 165 - 173*

The authors discuss how to translate RPCs securely between different distributed file systems with reference to a prototype NFS to DFS translator, and give protocol details.

032424 'Paving the Road to Internet Security or the Value of Small Cobblestones'
H Orman, S O'Malley, R Schroeppel, D Schwartz, *ISOC 94 pp 53 - 65*

The authors report experiments with minimalist crypto protocols. These include network layer packet encryption, and minimality is achieved at the cost of having no options; thus all hosts in a protection domain must be configured similarly, although non-local traffic can be handled differently. Interaction with Kerberos is discussed.

032425 'The European PASSWORD Project: A Status Report'
M Roe, *ISOC 94 p 47*

The author describes an EC project to pilot authentication and security services; PEM, X.400 and X.500 were implemented separately by UK, French and German researchers, and this helped to find and fix ambiguities in the standards documents. The project has concluded that the PEM certification hierarchy is unworkable, as it assumes that a single orgnanisation can be trusted to control the entire world's key distribution system.

032426 'Proof of Soundness (Integrity) of Cryptographic Protocols'
GJ Simmons, *Journal of cryptology v 7 no 2 (Spring 1994) pp 69 - 77*

The author discusses protocol failures in cryptographic protocols and the resulting motivation for the use of formal methods; Meadows' Oakland 91 paper was a good example of the power of such approaches. As test cases for formal tools, he puts forward broken protocols by Purdy-Simmons-Studier and Tatebayashi-Matsuzakai-Newman; he also discusses the 1990 Oberwolfach meeting on the subject.

032427 'Backward State Analysis of Cryptographic Protocols Using Coloured Petri Nets'
DM Stal, SE Tavares, H Meijer, *SAC 94 pp 107 - 118*

The authors use Petri nets to model intruders in protocols and to search for insecure states; they use this to analyse protocols by Hwang and ISO, and give net models in some details. A possible weakness is displayed in one of these.

032428 'Formal Requirements for Key Distribution Protocols'
R Syverson, C Meadows, *Eurocrypt 94 pp 325 - 337*

The authors construct a requirements definition language based on temporal logic, and apply it to a modified Newman-Stubblebine reauthentication protocol. They find an implementation dependent flaw, in which an initiator may accept part of a time stamp for a key, and also a place where the requirements may have been too stringent. This approach provides both a means to specify requirements and a chance to find flaws either in the protocol or requirements.

032429 'On Unifying Some Cryptographic Protocol Logics'
PF Syverson, PC van Oorschot, *Oakland 94 pp 14 - 28*

The authors present an evolute of the BAN logic whose goal is to subsume the extensions of Gong-Needham-Yahalom, Abadi-Tuttle and van Oorschot. It can cope with Diffie-Hellman key agreement and with the reception and comprehension of messages; it also has a model theoretic formal semantics.

032430 'CA-browsing system - a supporting application for global security services'
T Trček, T Klobučor, B Jerman-Blačič, F Bračan, *ISOC 94 pp 123 - 128*

The authors have constructed a tool for examining the structure of certification paths under X.500. It is based on an adjacency matrix, and uses either Dijkstra's or Pollack's algorithm to find a short path between two users. This approach is successful where there is a systematic CA structure, or a lot of cross-certificates.

032431 'On the Security Verification of the Authentication Protocol Kerberos'
H Watanabe, T Fujiwara, T Takata, T Kasami, *SCIS 94 paper 1A (in Japanese)*

The authors present a method for analysing protocols to see whether they leak session keys. They verified the Kerberos protocol using this method.

032432 'Authentication in the TAOS Operating System'
E Wobber, M Abadi, M Burrows, B Lampson, *ACM Transactions on Computer Systems v 12 no 1 (Feb 1994) pp 3 - 32*

The authors describe the design and implementation of the cryptographic protocols in an experimental distributed operating system. These support not just the authentication of principals, but also groups, rôles and delegation; the mechanism, which has been formally verified, consists of credentials built up from certificates. The notion of identity is built in at a very low level and kept consistent everywhere; a simple API represents the principles which a process can speak for. The heart of the system is a server which manages the credentials, although the use of the on-line service is minimised to keep things scalable.

032433 'Trust-based Navigation in Distributed Systems'
R Yahalom, B Klein, T Beth, *Computing Systems Usenix v 7 no 1 (Winter 1994) pp 45 - 73*

The authors introduce a logic for reasoning about trust relationships in distributed systems, and particularly about chains of certification of public keys; they give an algorithm for searching for a certification path between two known entities.

5 Secret Key Algorithms

032501 'Simple and Effective Key Scheduling for Symmetric Ciphers'
CM Adams, *SAC 94 pp 129 - 133*
The author proposes a key scheduling technique for substitution permutation networks, which uses S-boxes in the key schedule itself to eliminate weak and semi-weak keys.

032502 'On Matsui's linear cryptanalysis'
E Biham, *Eurocrypt 94 pp 349 - 361*
The author compares and discusses the mechanisms of differential and linear cryptanalysis. It is shown that their formal structure is similar; characteristics can be defined similarly, but the concatenation rule differs. This analysis leads to constraints on the size of the S-boxes in DES; the input must not be exponentially larger than the output, or highly probable characteristics are inevitable. Also, a known plaintext attack on Feal-8 is given which is better than that of Matsui and Yamagishi.

032503 'The divisors of $x^{2^m} + x$ of constant derivatives and degree 2^{m-2}'
C Carlet, *SIAM Journal of Discrete Mathematics v 7 no 2 (May 94) pp 238 - 244*
Those polynomials of degree 2^{m-2} over $GF(2^m)$ which divide $x^{2^m} + x$, and whose derivatives are constant, are affine. These are the locator polynomials of codewords of weight $2^{m-2} - 1$ of the BCH code of design distance $2^{m-2} - 1$; an explicit construction is given for them.

032504 'Links between differential and linear cryptanalysis'
F Chabaud, S Vaudenay, *Eurocrypt 94 pp 363 - 374*
The paper defines two functions $D(F)$ and $\triangle(F)$ which measure the resistance of functions $F : GF(2)^p \rightarrow GF(2)^q$ to the techniques of differential and linear cryptanalysis, respectively. The goal is to find functions F which give the best resistance under these measures. It turns out that almost perfect nonlinear functions are relevant; the authors define a notion of an almost bent function, which is also relevant.

032505 'Maximal and Near-Maximal Shift Register Sequences: Efficient Event Counters and Easy Discrete Logarithms'
DW Clark, LJ Weng, *IEEE Transactions on Computers v 43 no 5 (May 94) pp 560 - 568*
Reducible trinomials can be useful: if we want a 32-bit generator, for example, we find that there is no primitive trinomial of degree 32 over $GF(2)$, but $x^{32} + x^{15} + 1$ has a period which is 99.95% of the maximum. The authors prove that a polynomial will have a period of at least half the maximum if and only if it has no linear or repeated factors, its irreducible factors are all primitive, and the degrees of these irreducible factors are pairwise relatively prime. Furthermore, these polynomials will tend to have smooth periods, which facilitates discrete log calculations.

032506 'On the lattice structure of certain linear congruential sequences related to AWC/SWB generators'
R Couture, P L'Ecuyer, *Mathematics of Computation v 62 no 206 (April 1994) pp 799 - 808*
The authors analyse congruential generators recently introduced by Marsaglia, Zaman and others. They show that these all have a bad lattice structure, and that short vectors in their lattices can be found even when the modulus is very large.

032507 'Orientable Sequences'
ZD Dai, KM Martin, MJB Robshaw, PR Wild, *Cirencester III pp 97 - 115*
The periods of sequences which are orientable, in the sense that no n bit subsequence and its reverse occur more than once, have an upper bound $U = 2^{n-1} - 2^{(n+1)/2}$ and lower bound $L = 2^{n-1} - \frac{n}{4}(2^{(n+1)/2} + 2^{\lfloor \frac{n}{2} \rfloor} - 4) - 1$; these two expressions have the property that $(U - L)/L \rightarrow 0$ as $n \rightarrow \infty$.

032508 'New information on the history of the Siemens and Halske T52 cipher machines'
DW Davies, *Cryptologia v XVIII no 2 (April 1994) pp 141 - 146*

The author discusses the mechanisms used to step the rotors in the later versions of the T52. Previous published papers on this topic may have described a post-war Norwegian modification of the mechanism.

032509 'Linearity in block ciphers'
EP Dawson, LJ O'Connor, HM Gustafson, *SAC 94 pp 59 - 69*

The authors discuss the linear relationships which underly differential and linear attacks, which are briefly explained. They point out that as enumeration properties are asymptotic, is it quite possible to select S-boxes which possess them and which are nonetheless weak.

032510 'Explicit inversive congruential pseudorandom numbers with power of two modulus'
J Eichanauer-Herrmann, K Lekstadt, *Mathematics of Computation v 62 no 206 (April 1994) pp 787 - 797*

For the inversive generator given by $y_n = (an+b)^{-1} (\text{mod } 2^m)$, the authors provide upper and lower bounds on the discrepancy of pairs of outputs. However, they also show that it fails the serial test for k-tuples with $K \geq 3$.

032511 'Improved lower bounds for the discrepancy of inversive congruential pseudorandom numbers'
J Eichanauer-Herrmann, *Mathematics of Computation v 62 no 206 (April 1994) pp 783 - 786*

The author gives improved bounds on the discrepancy of k-tuples, from an inversive congruential generator with a prime modulus, which uses a simplified proof technique.

032512 'Embedding and probabilistic correlation attacks on clock-controlled shift registers'
JD Golić, L O'Connor, *Eurocrypt 94 pp 231 - 243*

Embedding and correlation attacks on clock-controlled binary shift registers (with not necessarily linear feedback) which are clocked at least once per output symbol are defined and analyzed. The attack efficiency is described in terms of the capacity of the corresponding communication channel; in addition to improving some previous bounds, the authors derive the minimum lengths of sequence which are vulnerable to various types of embedding attack. Higher decimation rates can make practical attacks harder, but do not improve the theoretical security,

032513 'Transformation Matrices of Clock-Controlled Shift Registers'
D Gollmann, *Cirencester III pp 197 - 210*

The author examines the distribution of k-tuples in clock controlled sequences, and shows that their distribution becomes more uniform as the length of the cascade increases. Experimentally, this convergence proceeds even faster than one expects from a naïve analysis, and sharper bounds can be found by examining the spectra of the transformation matrices. This led to the discovery of a neat attack on cascades of registers of length 3.

032514 'Feedback registers based on ramified extensions of the 2-adic numbers'
M Goresky, A Klapper, *Eurocrypt 94 pp 211 - 223*

The authors introduce a new type of nonlinear feedback shift register, namely ramified feedback-with-carry shift registers (or d-FCSRs, where d is the ramification). The algebraic structure of the sequences generated by d-FCSRs is completely parallel to the structure of linear feedback shift registers; sequences generated by d-FCSRs with d = 1 have also been studied. As an application of their work, the authors show that certain combiners with memory, including the summation cipher, are insecure.

032515 'A general lower bound for the linear complexity of the product of shift-register sequences'
R Göttfert, H Niederreiter, *Eurocrypt 94 pp 225 - 230*

The authors give a lower bound for the linear complexity of the termwise product of any two linear shift register sequences. Their result also gives information on the minimal polynomial of such a product; sometimes the lower bound gives the actual linear complexity.

032516 'Key Clustering and Substitution-Permutation Network Cryptosystems'
HM Heys, SE Tavares, *SAC 94 pp 134 - 145*

Substitution permutation networks may have keys which cluster, in the sense that keys which are close in Hamming distance may generate ciphertexts with the same property. To prevent this, a key avalanche criterion is introduced, and its theoretical parameters are developed. Empirical tests on substitution permutation networks with various numbers of rounds are reported.

032517 'A Practical Attack against Knapsack based Hash Functions'
A Joux, L Granboulan, *Eurocrypt 94 pp 61 - 70*

The authors attack Damgård's knapsack hash function by showing how to reduce collision search to lattice basis reduction (whether LLL or the Schnorr-Euchner variant of Korkine-Zolotarev). They found a collision for a 120-bit hash function in 3 hours, and provide timings for smaller examples.

032518 'DES Can Be Immune to Linear Cryptanalysis'
KJ Kim, SJ Lee, SJ Park, DK Lee, *SAC 94 pp 70 - 81*

The authors had previously suggested that $S(x) \neq S(x \oplus 11ef10)$ would strengthen the DES S-boxes against linear attacks. In response to comment, they consider four round linear approximations and derive additional constraints on the S-box ordering; other design constraints are also suggested.

032519 'Classification of Hadamard matrices of order 28 with Hall sets'
H Kimura, *DIscrete Mathematics v 128 (April 94) pp 257 - 268*

The author shows that there are exactly 486 inequivalent Hadamard matrices of order 28 with Hall sets.

032520 'Cryptanalysis of LOKI'
LR Knudsen, *Cirencester III pp 223 - 236*

The author shows that any LOKI key K has the same effect as k xor $hhh...$ where $hhh...$ is any hex digit repeated 16 times. Thus when LOKI is used as a hash function, collisions are easy to find. he also shows that one can use 3-round characteristics plus fixed points to construct a 2^{51} differential attack on a 13 round version of the algorithm.

032521 'Some new weighing matrices using sequences with zero autocorrelation function'
C Koukouvinos, J Seberry, *Australasian Journal of Combinatorics v 8 (Sep 93) pp 143 - 152*

The authors prove the skew weighing conjecture for orders $2^t.13$, $t \geq 5$, and $2^t.15$, $t \geq 3$. They also provide tables of sequences of length 13 and 15 whose periodic (or nonperiodic) autocorrelation functions are zero.

032522 'On the Relation of Matsuis Method and Differential Equation Method for FEAL'
T Masuda, T Kaneko, *SCIS 94 paper 4B (in Japanese)*

The authors contrast the expected cost of two techniques (due to Matsui and to Kaneko et al respectively) for attacking the FEAL cryptosystem. The analysis may find application to other Feistel-like cryptosystems.

032523 'On correlation between the order of S-boxes and the strength of DES'
M Matsui, *Eurocrypt 94 pp 377 - 387*

The author studies the duality between his method of linear cryptanalysis and the Biham-Shamir method of differential cryptanalysis. Biham and Shamir observed that changing the order in which the S-boxes are used in DES usually weakens DES with respect to differential cryptanalysis; but the author shows that such a change usually strengthens DES with respect to linear cryptanalysis.

032524 'A New Cryptanalytic Method for FEAL Cipher'
M Matsui, A Yamagishi, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 2–7*

In this paper, the authors propose a new known-plaintext attack on the FEAL cipher. The method is a kind of meet-in-the-middle attack with a partial exhaustive key search, and can derive all possible key candidates directly and in a deterministic way. As a result, it is possible to break FEAL-4 and FEAL-6 with 5 and 100 known plaintexts respectively. The authors also show a method to break FEAL-8 with 2^{15} known plaintexts.

032525 'A note on the combination of compression and encryption'
S Matsuoka, M Morii, H Nakano, *SCIS 94 paper 8C (in Japanese)*

The authors propose a communication protocol that combines Huffman Coding for compression with the FEAL cryptosystem; they then examine the security of such a protocol.

032526 'A Low Cost, High Speed Encryption System and Method'
GL Mayhew, *Oakland 94 pp 147 - 154*

The author presents a stream cipher used by Hughes Aircraft in commercial and military products. In a typical configuration, it consists of a 61 bit shift register and eight 6-to-1 bit nonlinear filter functions, which together provide one byte of keystream at each clock tick. The base key is the shift register's feedback polynomial, and the message key is its initial state.

032527 'Weight class distributions of de Bruijn sequences'
GL Mayhew, *Discrete Mathematics v 126 (March 94) pp 425 - 429*

The author counts the de Bruijn sequences of order 6 and 7 (ie of length 2^6 and 2^7 by weight class (the Hamming weight of the generating function). He conjectures that the largest power of 2 which divides the number of sequences in each weight class is the cardinality of a symmetry group that operates on all the weight classes of that order.

032528 'Randomness Properties of Two Chaotic Mappings'
A McGrail, *Cirencester III pp 265 - 295*

The author reports extensive empirical tests of chaotic sequences. Hénon sequences are poor pseudorandom generators, but adding five of them together appears to solve the problem.

032529 'The self-shrinking generator'
W Meier, O Staffelbach, *Eurocrypt 94 pp 201 - 210*

At Crypto 93, Coppersmith, Krawczyk and Mansour introduced a pseudorandom sequence generator, based on two linear feedback shift registers, which they called the shrinking generator. The authors introduce a closely related but in some ways simpler generator which uses only one shift register. This has the advantage that it allows implementation of the shrinking principle with less hardware.

032530 'Fast Attacks on Tree-structured Ciphers'
W Millan, EP Dawson, LJ O'Connor, *SAC 94 pp 146 - 158*

Tree-structured ciphers, which range from some self-synchronising stream ciphers to Kam and Davida's SP-networks, are open to the reconstruction attacks introduced by Anderson and others. In the present paper, the writers develop the technique further; they show that information about the nonlinear structure of unknown nodes can make the attack several times faster, and that even a small number of chosen texts can be enough to unravel an unknown permutation in the middle of such a structure. These results extend the attack on Kühn's cipher.

032531 'New Proposal and Comparison of Closure Tests - More Efficient than the CRYPTO'92 Test for DES'
H Morita, K Ohta, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 15–19*

The authors extend the Switching Closure Test, a successor of the meet-in-the-middle closure test, to DES-like cryptosystems. They show that this variant is more efficient than the closure test proposed by Campbell and Wiener at Crypto '92, in that it establishes a better relationship between the amount of computation and the probability of error.

032532 'Image Scrambling Scheme Employing a Dyadic Shift'
N Naitoh, *SCIS 94 paper 7A (in Japanese)*

This paper proposes an image scrambling system that might be used in a pay-per-view television system.

032533 'A Study on the Differential Attack for MBAL Cryptosystem'
K Noguchi, H Ashiya, Y Sano, T Kaneko, *SCIS 94 paper 14B (in Japanese)*

The authors examines a recently proposed cryptosystem called MBAL, and finds a usable differential characteristic with probability 2^{-15}.

032534 'Designing Product Ciphers using Markov Chains'
L O'Connor, *SAC 94 pp 2 - 13*

The author discusses using Markov methods to estimate the number of rounds a block cipher needs in order to be secure against differential and linear attacks. Although simple to state, this technique can be hard to apply; some details of its use are described. Ergodic theory and random graph theory may also be relevant to this problem.

032535 'Message Authentication Codes and Differential Attack'
K Ohta, M Matsui, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 8–14*

This paper discusses the security of MAC schemes from the viewpoint of differential attacks. The authors propose an attack that is effective against DES-MAC and FEAL-MAC, and estimate the number of appropriate plaintext pairs needed to derive the secret key.

032536 'Linear Approximation Versus Nonlinearity'
J Pieprzyk, C Charnes, J Seberry, *SAC 94 pp 82 - 90*

The authors discuss the mechanics of linear cryptanalysis, and in particular how its use of linear approximation tables constrains the design of S-boxes.

032537 'Black Box Cryptanalysis of Hash Networks Based on Multipermutations'
CP Schnorr, S Vaudenay, *Eurocrypt 94 pp 51 - 60*

Where the boxes in an FFT network are given by oracles, bounds can be given on the effort required to find collisions or invert output values. In real designs, these black boxes may be multipermutations constructed from binary operations.

032538 'How to Better the SAC'
J Seberry, XM Zhang, YL Zheng, *SAC 94 pp 52 - 58*

Functions which do not satisfy the strict avalanche criterion can often be fixed by multiplying the input by a suitable matrix (see below). This technique can be used to construct functions on successively more variables which satisfy this criterion.

032539 'Improving the strict avalanche characteristics of cryptographic functions'
J Seberry, XM Zhang, Y Zheng, *Information Processing Letters v 50 no 1 (8/4/94) pp 37 - 42*

The authors show how to 'repair' boolean functions with inadequate avalanche properties by doing a linear transformation on their inputs. If f is the function, and $f(x) \oplus f(x \oplus \gamma_i)$ is balanced for each row γ_i of a nondegenerate matrix A, then $f(xA)$ will satisfy the strict avalanche criterion.

032540 'Nonlinearity Characteristics of Quadratic Substitution Boxes'
J Seberry, XM Zhang, YL Zheng, *SAC 94 pp 14 - 29*
Quadratic S-boxes have a number of close relationships between differential uniformity, nonlinearity and avalanche criteria. These are discussed, and it is shown that there exists no differentially 2-uniform quadratic permutation on an even dimensional vector space.

032541 'Relationships among nonlinearity criteria'
J Seberry, XM Zhang, Y Zheng, *Eurocrypt 94 pp 389 - 401*
An S-box all of whose component Boolean functions are quadratic is called a quadratic S-box. The authors prove a lower bound on the nonlinearity of these. For quadratic S-boxes which have an additional desirable property called regularity, the authors prove some relationships among various properties of such an S-box, such as satisfying avalanche criteria or possessing linear structures.

032542 'The Norwegian modification of the Siemens and Halske T52e cipher machines'
E Selmer, *Cryptologia v XVIII no 2 (April 1994) pp 147 - 149*
The author describes modifying captures Siemens T52e encrypting teleprinters for use by Norwegian security police in 1946. They remained in use until about 1960.

032543 'On Some Applications of Finitely Generated Semigroups'
IE Shparlinksi, *ANTS 94*
The author uses bounds for character sums to get results on the distribution of the residues mod q of a multiplicative semigroup. This has consequences for the quality of congruential generators.

032544 'On a Cipher Evaluation Method Based on Differential Cryptanalysis (II)'
T Sorimachi, T Tokita, M Matsui, *SCIS 94 paper 4C (in Japanese)*
Effective use of differential cryptanalysis relies upon finding a characteristic of a cryptosystem that may be exploited at minimum cost. The authors show that a single cryptosystem (in this case DES) may be used in various different ways each of which has a different minimum cost characteristic, and present a new characteristic for several modes of DES.

032545 'Provably Good Pattern Generators for a Random Pattern Test'
TH Spencer, *Algorithmica v 11 no 5 (March 94) pp 429 - 442*
Linear shift register sequences have a number of undesirable local properties which can be removed by simply adding a random constant to their output.

032546 'Recent Results on Resilient Functions'
DR Stinson, *SAC 94 pp 30 - 39*
An (n, m, t) resilient function is an n-to-m bit function with the property that even when t of its input bits are fixed, all m bit outputs are still equiprobable. Recent results are reviewed, including that such functions are equivalent to large sets of orthogonal arrays $OA_{2^{n-m-t}}(t, n, 2)$ and to the existence of $(n, m, t+1)$-codes; and that conversely, for all $r > 3$, codes can be used to construct resilient functions with parameters $(2^{r+1}, 2r+2, 2^r - 2^{(r-1)/2} - 1)$ and $(2^{r+1}, 2^{r+1} - 2r - 2, 5)$.

032547 'The k-dimensional distribution of combined GFSR sequences'
S Tezuka, *Mathematics of Computation v 62 no 206 (April 1994) pp 809 - 817*
The author shows how to apply lattice techniques to analyse sequences which are the bitwise exclusive-or of a number of general feedback shift register systems. In particular, the twisted GFSR sequences of Matsumoto and Kurita can be unravelled using Couture's theorem.

032548 'A method to generate autocorrelated uniform random numbers'
TR Willemain, PA Desautels, *Journal of Stat. Comp. Simul. v 45 no 1 - 2 pp 23 - 31*
The authors propose a 'sum of uniforms' method in which uncorrelated random numbers are added pairwise and then transformed to a uniform distribution. This transformed sum is then used as one of the two components of the next sum.

032549 'Information Leakage of Boolean Functions as a Measure of Cryptographic Strength'
M Zhang, SE Tavares, LL Campbell, *SAC 94 pp 40 - 51*

The authors define static and dynamic information leakage in an S-box as 1 - $H(Y \mid X\text{fixed})$ and 1 - $H(\triangle Y \mid \triangle X\text{fixed})$ respectively. They prove a number of results, including links with correlation immunity and resilience, and discuss the tradeoffs between information leakage and avalanche properties.

032550 'Universal circuit matrix for adjacency graphs of feedback functions'
J Żurawiecki, *Discrete Mathematics v 126 (Mar 94) pp 441 - 445*

The author introduces a matrix which transforms the feedback function of a de Bruijn sequence into the circuit matrix of the related adjacency graph.

6 Public Key Algorithms

032601 'Privacy and Authentication for Wireless Local Area Networks'
A Aziz, W Diffie, *IEEE Personal Communications v 1 no 1 (Q1 94) pp 25 - 31*
The authors present a protocol for the air link of wireless LANs between mobile units and a base station. This includes features such as dynamic negotiation of the bulk encryption algorithm, support for multiple certification authorities, and the fact that compromise of a mobile's secrets will not leak previous sessions. A security analysis is given using the BAN logic.

032602 'Space Requirements for Broadcast Encryption'
C Blundo, A Cresti, *Eurocrypt 94 pp 291 - 301*
The authors consider schemes in which each client has some secret keys, and the server broadcasts a session key for use by a designated subset of clients. They use the concept of zero-message broadcast to show that the Fiat-Naor scheme is optimal in the sense of requiring number of keys for resilience against a given number of conspiring clients. However, if clients can interact while computing the session key, this lower bound can be beaten.

032603 'Comment: New digital signature scheme based on discrete logarithm'
C Boyd, *Electronics Letters v 30 no 6 (17th March 94) pp 480 - 481*
The author remarks that a recent scheme of Yen and Laih has the weakness that any number of signed messages can be generated from a known public key, and that the signature of a message congruent to zero (mod q) will be equal to the signer's secret key. He concludes that a one-way hash function is needed.

032604 'Multisignatures Revisited'
C Boyd, *Cirencester III pp 21 - 30*
A scheme is presented which extends Fiat-Shamir signatures to two signers, and which can be generalised to larger groups without difficulty. The secret key of the group ends up as the componentwise product of the keys of each signatory.

032605 'A Secure and Efficient Conference Key Distribution System'
M Burmester, Y Desmedt, *Eurocrypt 94 pp 279 - 290*
Ingemarsson, Tang, and Wong designed a conference key distribution system based on symmetric functions, which was later shown to be insecure. The authors present an improved version based on cyclic functions, which resists both active and passive attacks provided that the Diffie-Hellman problem is hard. The communications and computations are evenly apportioned among the participants, and versions with and without broadcast are described. A public key system, with proof of security against a known plaintext attack, is used for authentication.

032606 'On the security of some cryptosystems based on error-correcting codes'
F Chaubaud, *Eurocrypt 94 pp 127 - 135*
The author examines public key systems based on coding theory, and in particular those of McEliece and Stern. He studies their vulnerability to the available decoding algorithms, and derives lower bounds on the parameter sizes.

032607 'Designated Confirmer Signatures'
D Chaum, *Eurocrypt 94 pp 95 - 101*
The author introduces signatures which can be checked only by a designated person, and which come with a protocol by which the signer can convince the recipient that this person will in fact be able to perform this verification.

032608 'Identity-based conference key broadcast schemes with user authentication'
JL Chen, TNL Hwang, *Computers and Security v 13 no 1 (Feb 1994) pp 53 - 57*
The authors extend the Maurer-Yacobi identity-based scheme to provide two identity-based conference key schemes. These depend on a modulus being too large to factor, but whose factors are small enough that someone who knows them can calculate discrete logs.

032609 ‘New Group Signature Schemes’
L Chen, TP Pedersen, *Eurocrypt 94 pp 163 - 173*

Group signature schemes let members sign messages anonymously on behalf of a group, and two such schemes are shown. In one of these, the anonymity becomes unconditional, while the second is more efficient than previous systems with only computational security; both can be arranged so that any sufficiently large set of group members can identify the signer.

032610 ‘Methodology for digital money based on general cryptographic tools’
S D’Amiano, G Di Crescenzo, *Eurocrypt 94 pp 151 - 162*

The authors show how digital cash schemes might be based on zero knowledge and oblivious authentication. However, detecting multiple spending means using a broadcast protocol in which the bank requests anyone who has handled a copy of the offending coin to prove their honesty.

032611 ‘Multisignature Scheme with Specified Order’
H Doi, E Okamoto, M Mambo, T Uyematsu, *SCIS 94 paper 3A (in Japanese)*

The authors contrast signature schemes in which multiple signatures are required. For some applications the order in which signing takes place is unimportant, but sometimes it is important. The paper presents schemes of both types based on RSA.

032612 ‘Single-Term Divisible Electronic Coins’
T Eng, T Okamoto, *Eurocrypt 94 pp 313 - 323*

Ferguson and Brands presented efficient digital cash systems in 1993, while the 1991 scheme by Okamoto and Ohta was less efficient but had divisible digital coins: consumers were permitted to re-spend parts of a coin up to the fixed total. The scheme proposed here combines the desirable features of both; it uses restricted blind signatures, a binary tree approach to divisibility, and a three move protocol for disposable authentication. Its security is based on the discrete logarithm problem.

032613 ‘New digital signature scheme based on discrete logarithm’
L Harn, *Electronics Letters v 30 no 5 (3 March 94) pp 396 - 398*

The author proposes that a user with secret key x and public key $y = g^x \pmod p$ should sign a message m as (r, s) where $r = g^k \pmod p$ for a random message key k, and $s = x(r + h(m)) - k \pmod{p-1}$. This can be adapted to multisignatures, with signatures and public keys combined by $r = \prod r_i$, $s = \sum s_i$ and $y = \prod y_i$.

032614 ‘Threshold cryptosystem with multiple secret sharing policies’
L Harn, HY Yin, S Yang, *IEEE Transactions on Computers and Digital Techniques v 141 no 2 (Mar 94) pp 142 - 144*

The authors propose a threshold cryptosystem for use with discrete log based encryption. It is based on Lagrange interpolation and the representation problem.

032615 ‘Electronic Anonymous Bidding Schemes’
Y Imamura, T Matsumoto, H Imai, *SCIS 94 paper 11B (in Japanese)*

Bidding strategies differ according to whether an auction is ”blind” or open. If the bids from a blind auction are revealed after the event then this may aid bidders wishing to collude in a subsequent auction. The authors propose a bidding scheme in which the identities of bidders remain secret following the auction.

032616 ‘Secure Addition Sequence and Its Applications on the Server-Aided Secret Computation Protocols’
CS Laih, SM Yen, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 81–88*

In this paper, the authors extend the concept of addition sequence to the secure addition sequence, and develop an efficient algorithm to construct such sequences. The performance of server-aided secret computation protocols may be enhanced by incorporating such sequences.

032617 '(t,n) Threshold Signature Schemes Based on Discrete Logarithm'
CM Li, TNL Hwang, NY Lee, *Eurocrypt 94 pp 191 - 200*

Many threshold schemes have the property that if more than the threshold number of participants collude, they can derive the center secret. The authors seek to prevent this by blinding the individual secrets; they produce two schemes, one with and one without a trusted dealer, which thus appear to resist collusion attacks.

032618 'An Electronic Payment System with Distributed Control'
T Matsumoto, *SCIS 94 paper 16A (in Japanese)*

This paper proposes an electronic payment system, using smart-cards and intelligent electronic "mediators" to minimise communication with the central authority. A non-realtime link is used to reduce the abuses that are found in entirely off-line systems.

032619 'Elliptic Curves Suitable for Cryptosystems'
A Miyaji, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 98–105*

In this paper, the author investigates how one can construct elliptic curves suitable for cryptosystems that use smaller keys and less computation without compromising security. He also shows the advantages of these curves in the case of Schnorr's digital signature scheme.

032620 'A structure of the system using personal computers for multiple electronic approval'
Y Murata, T Saito, S Miyaguchi, *SCIS 94 paper 11E (in Japanese)*

This paper proposes a system based upon the ESIGN digital signature scheme that may be used to sign documents for which multiple independent signatures are necessary and simple general-purpose computers must be used.

032621 'Remarks on the LUC public key system'
S Murphy, *Electronics Letters v 30 no 7 (31 March 94) pp 558 - 559*

The author provides much shortened proofs of the results underlying the LUC public key system, and points out that the original proof does not hold for characteristic two.

032622 'Can DSA be Improved? - Complexity Trade-Offs With the Digital Signature Standard'
D Naccache, D M'Raïhi, D Raphaeli, S Vaudenay, *Eurocrypt 94 pp 85 - 94*

The authors show various ways in which DSA signatures can be optimised for smartcard applications. These include two ways of batching transactions, transferring the modular division from the signer to the verifier, signer-aided compressed signatures, and the use of precomputed coupons.

032623 'Comment: New digital signature scheme based on discrete logarithm'
K Nyberg, *Electronics Letters v 30 no 6 (17th March 94) pp 480 - 481*

The author shows that in the Yen-Laih signature scheme it is possible to transform any (message, signature) pair into another valid pair in a large number of ways. She concludes that a hash function must be used with this scheme.

032624 'Message Recovery for Signature Schemes Based on the Discrete Logarithm problem'
K Nyberg, RA Rueppel, *Eurocrypt 94 pp 175 - 190*

The authors develop their previous results to show that not just the DSA, but all ElGamal type schemes, have variants giving message recovery: the basic idea is to turn the scheme round so that the message appears as a group element, rather than in an exponent. They discuss a number of variant schemes with differing computational and other properties.

032625 'A Multiple-Iterated Trapdoor For Dense Compact Knapsacks'
G Orton, *Eurocrypt 94 pp 115 - 126*

The author shows how the density of a multiply iterated knapsack can be made to approach 1, by introducing extra weights at intermediate rounds. He argues that the resulting system should resist lattice based attacks.

032626 'Digital Signatures: RSA or El Gamal?'
F Piper, N Stephens, *Cirencester III pp 311 - 319*
The authors propose a trapdoor in prime number generators for use with RSA - the primes would be chosen randomly from a large stored list. More practically, a linear combination of elements from shorter lists might be used as a starting point for a search.

032627 'Breaking an Efficient Anonymous Channel'
B Pfitzmann, *Eurocrypt 94 pp 339 - 348*
At Eurocrypt'93, Park, Itoh, and Kurosawa presented two efficient designs for an anonymous channel based on Chaum's mix-nets. The idea was to simulate a trusted host for applications like electronic voting with secret inputs and public outputs. Here, the author first identifies a passive attack against both designs that may allow correlation of inputs and outputs, and shows how to avoid this by careful choice of parameters. She then demonstrates an active attack was proposed that completely breaks one of the designs; there may be ways to avoid this attack on the other design by adding counters and redundancy.

032628 'Comments on "Cryptanalysis of Knapsack Ciphers Using Genetic Algorithms" '
F Rubin, *Cryptologia v XVIII no 2 (April 1994) pp 153 - 154*
The author criticises Spillman's use of genetic algorithms to attack knapsack ciphers (**024621**) as ineffective against the kind of knapsacks actually proposed for nontrivial cryptographic use.

032629 'New Key Generation Algorithm for RSA Cryptosystem'
R Sakai, M Morii, M Kasahara, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 89–97*
This paper presents a new algorithm for generating RSA keys that are secure against Wiener's attack, together with a variant for generating strong keys, and the performance of these algorithms is analyzed.

032630 'Electronic Voting Scheme Allowing Open Objection To the Tally'
K Sako, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 24–30*
This paper presents an electronic voting scheme, which allows a valid voter to make an open objection to the centre without making public what he has voted. It has a single voting centre with an anonymous channel, and uses a 3-move protocol between each voter and the centre, with one extra move if one wants to object to the tally.

032631 'Subliminal Channels for Transferring Signatures: Yet Another Cryptographic Primitive'
K Sakurai, T Itoh, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 31–38*
This paper explores the transfer of signatures using the subliminal channels in the parallel version of the Fiat-Shamir identification scheme. It introduces a new notion, the 'privately recordable signature' which is generated by the interactive protocol between the signer and the verifier, and only the verifier can keep the signature (no third party can record it). In this scheme, the disclosure of the verifier's private coin turns the signature into an ordinary digital signature which can be verified with the signer's public key.

032632 'Secret Sharing'
B Schneier, *PC Techniques v 5 n 2 (Jun 94) pp 24 - 30*
An introduction to threshold schemes, this article discusses the basic theory, implementations, and applications. It includes C source code for the Lagrange interpolating polynomial scheme.

032633 'Subliminal Channels in the Digital Signature Algorithm'
B Schneier, *PC Techniques v 5 n 2 (Jun 94) pp 72 - 76*

The Digital Signature Algorithm has several subliminal channels, covert communication channels that a signer can use to send a message to a specific receiver. These subliminal channels are described and discussed in this article.

032634 'Distributed assignment of cryptographic keys for access control in a hierarchy'
BM Shao, JJ Hwang, PC Wang, *Computers and Security v 13 no 1 (Feb 1994) pp 79 - 84*

The authors put forward a public-key variant of the Akl-Taylor scheme for key hierarchies, and discuss its use in distributed systems.

032635 'Multisignature Schemes Based on the ElGamal Scheme'
A Shimbo *SCIS 94 paper 3C (in Japanese)*

The paper describes several multisignature schemes which differ in the number of messages required. The author contrasts single pass protocols with round robin multiple pass protocols.

032636 'Identity-Based Non-interactive Key Sharing'
H Tanaka, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 20–23*

This paper proposes a new identity-based non-interactive key sharing scheme in order to realise the original concept of an identity-based cryptosystem. The security of the new scheme depends on the difficulty of factoring. The author also considers the necessary conditions for secure realization of identity-based non-interactive key sharing schemes.

032637 'Knapsack Cryptosystem using Partial Superincreasing Vector'
A Tanaka, K Kobayashi, *SCIS 94 paper 10C (in Japanese)*

The authors propose a hybrid cryptosystem based on the knapsack problem. The paper claims that the system is secure against attacks based on lattice basis reduction, and suggests that breaking it is NP hard.

032638 'A technique for remote authentication'
WA Wulf, A Yasinac, KS Oliver, R Peri, *ISOC 94 pp 158 - 164*

The authors propose an authentication scheme based on the fact that modular exponentiation can be used to construct two one-way hash functions which commute.

032639 'An Off-line Credit Protocol for Inspection of Credit Limits'
K Yamamotoya, T Matsumoto, H Imai, *SCIS 94 paper 11C (in Japanese)*

This paper proposes a scheme by which credit checks may be performed off-line, so saving on communication costs. The protocol uses a "Super Smart Card" to prevent unauthorised transactions, such as a credit check without the knowledge of the customer.

032640 'How to Break and Repair Leighton and Micali's Key Agreement Protocol'
Y Zheng, *Eurocrypt 94 pp 303 - 309*

Leighton and Micali introduced a key distribution protocol at Crypto'93 based on tamper-proof hardware, a trusted smart card issuer, an authenticated public file, and a one-way hash function. This paper shows that the shared key computed by two parties will probably leak to many other participants; the suggested repair creates an identity-based system implemented with prefix-free encodings, and also yields storage and run-time improvements.

7 Computational Number Theory

032701 ‘The Function Field Sieve’
LM Adleman, *ANTS 94*

An analogue to the number field sieve is developed for calculating discrete logarithms over the finite field $GF(p^n)$. A heuristic analysis shows the running time to be subexponential, of order $L_{p^n}[1/3, c]$ for some $c > 0$, provided n is large enough relative to p.

032702 ‘A Subexponential Algorithm for Discrete Logarithms over the Rational Subgroup of Jacobians of Large Genus Hyperelliptic Curves over Finite Fields’
LM Adleman, J DeMarrais, MD Huang, *ANTS 94*

There are subexponential algorithms for finding discrete logarithms over finite fields. The authors give an algorithm for finding discrete logarithms in the group of rational points on the Jacobians of hyperelliptic curves. They present a heuristic argument that for hyperelliptic curves of sufficiently large genus, and for relatively small finite prime fields, their algorithm is subexponential. It is left as an open question whether their techniques could be applied successfully to elliptic curves.

032703 ‘Open Problems in Number Theoretic Complexity, II’
LM Adleman, KS McCurley, *ANTS 94*

This is a very useful catalogue of open problems, with remarks on progress since 1986, when the authors produced a similar list.

032704 ‘On the difficulty of finding reliable witnesses’
WR Alford, A Granville, C Pomerance, *ANTS 94*

If n is composite, let $w(n)$ denote the least positive integer such that n is not a strong pseudoprime to base $w(n)$. Thus $w(n)$ is a *witness* to the fact that n is composite. If an appropriate generalization of the Riemann Hypothesis is true, then $w(n) < 2\log^2 n$. Here the authors prove that for infinitely many n, $w(n) > (\log n)^{1/(4\log\log n)}$; in particular, this holds for infinitely many Carmichael numbers. They give an argument to suggest that the maximal order of $w(n)$ is $c\log n\log\log n$ for some constant $c > 0$, and under a version of the prime triplets conjecture they show that $w(n)$ has maximal order at least $c\log n$ for some constant $c > 0$.

032705 ‘Reducing Lattice Bases by Means of Approximations’
J Buchmann, *ANTS 94*

The author shows that both Korkine-Zolotarev and LLL reduction of a non-integer lattice can be done almost as quickly as for an integer lattice, and determine the precision necessary for the reduction of a rational approximation of a lattice basis to be useful.

032706 ‘Schoof’s algorithm and isogeny cycles’
JM Couveignes, F Morain, *ANTS 94*

The authors show how to use powers of ‘good’ small primes (in the sense of Elkies and Atkin) in an efficient way, to speed up the Schoof-Elkies-Atkin algorithm for counting the numbers of points on elliptic curves over a finite field. The second author has implemented these ideas, and presents details of the computation of the number of points on an elliptic curve over $GF(p)$, where p has 249 decimal digits.

032707 ‘Improved Bounds for the Rabin Primality Test’
I Damgård, P Landrock, *Cirencester III pp 117 - 128*

Let $p_{k,t}$ be the probability that a k-bit random number passes t rounds of the Rabin primality test. The authors improve previous results of Pomerance and others to show that, for example, $p_{256,6} \leq 2^{-51}$ and that for $k > 100$, $p_{k,t} \leq 4k2^{-\sqrt{k/2}}$. Explicit formulae are also given for various values of t, and consideration of the worst case numbers leads to the theorem that if n is odd and composite, and is a Rabin pseudoprime to more than an eighth of bases, then either n is divisible by 3, or $3n+1$ or $8n+1$ is a square, or n is a Carmichael number.

032708 'MIMD-factorisation on hypercubes'
F Damm, FP Heider, G Wambach, *Eurocrypt 94 pp 417 - 425*

The paper describes an implementation of the multiple polynomial quadratic sieve integer factorisation method on a 1024 processor MIMD computer. Using this, general 100 decimal digit integers can be factored in 1 or 2 days.

032709 'An analysis of the Gaussian algorithm for lattice reduction'
H Daudé, P Flajolet, B Vallée, *ATNS 94*

The authors present an analysis of the running time of Gaussian lattice reduction, which is supported by empirical data. On average, it has complexity $O(1)$; this explains why LLL runs much better in practice than its worst-case bound suggests.

032710 'Efficient exponentiation using precomputation and vector addition chains'
P de Rooij, *Eurocrypt 94 pp 405 - 415*

A new algorithm for exponentiation with precomputation in a given finite group is defined and analysed. Because of the precomputations, the exponentiation base should be fixed. The goal is to minimize the number of group operations needed for an exponentiation, without requiring too much precomputation or use of memory. The success of the new algorithm in these respects is compared with that of previous methods.

032711 'Factorization of Polynomials over Finite Fields in Subexponential Time under GRH'
S Evdokimov, *ANTS 94*

The author shows that, assuming the Generalized Riemann Hypothesis, there is a deterministic algorithm which will factorize a one-variable polynomial of degree n over the finite field with q elements in time $(n^{\log n} \log q)^{O(1)}$. The Generalized Riemann Hypothesis is used only to take roots in a finite field in polynomial time.

032712 'A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves'
G Frey, HG Rück, *Mathematics of Computation v 62 no 206 (April 1994) pp 865 - 874*

The authors extend the Menezes-Okamoto-Vanstone technique to groups associated with higher genus curves; in particular, they use the Tate pairing for Abelian varieties over local fields to reduce the discrete logarithm in the m-torsion part of the divisor class group to a simple discrete logarithm problem in an extension of the ground field.

032713 'Lattice sieving and trial division'
RA Golliver, AK Lenstra, KS McCurley, *ANTS 94*

The authors have achieved a substantial speed-up in the relation collection stage of the general number field sieve. They employ a new lattice sieving technique, and speed the trial division stage by a method based on lattice sieving in a hash table. Triple and quadruple large prime relations are collected efficiently. The authors also discuss parallelization of the algorithm. For a 129-digit number, they suggest that the necessary relations could be gathered in 1400 MIPS years.

032714 'Duality and Normal Basis Multiplication'
W Geiselmann, D Gollmann, *Cirencester III pp 187 - 195*

The authors show that using dual basis multiplication can facilitate the design of hardware multipliers in extension fields, and develop the necessary mathematics. This leads to a new interpretation of the Massey-Omura multiplier.

032715 'An acceleration of the Niederreiter factorisation algorithm in characteristic 2'
R Göttfert, *Mathematics of Computation v 62 no 206 (April 1994) pp 831 - 839*

the author explains in detail how Niederreiter's polynomial factoring algorithm works in characteristic 2, and describes a reduction technique which cuts the work factor to $O(dt^3 + d^e t^e + m^2 d (\log d)^2 (\log\log d) t (\log t) \log\log t)$ where $e < 2.38$ is the exponent of fast matrix multiplication in the field which has 2^t elements, and the polynomial which has degree d is assumed to have at most m factors.

032716 'On an Analysis of Legendre Subsequence'
K Hasegawa, M Hata, *SCIS 94 paper 9A (in Japanese)*

Let us assume that a pseudo-random sequence has as its kth element the Legendre symbol $(\frac{k}{p})$ for some prime p. The authors examine techniques for reconstructing the whole sequence from a part of it, and estimate the computational cost.

032717 'A Fast Variant of the Gaussian Reduction Algorithm'
M Kaib, *ANTS 94*

The author generalises a quadratic form algorithm of Schönhage to get a fast variant of Gaussian lattice reduction, which works for the l_1, l_2 and l_∞ norms.

032718 'Selection of a large sum-free subset in polynomial time'
MN Kolountzakis, *Information Processing Letters v 49 no 5 (11 March 94) pp 255 - 258*

A set of integers is called sum-free if $x + y \neq z$ for all x, y, z in it. An algorithm is given to extract a sum-free subset S from a set A in polynomial time such that $\mid S \mid > \mid A \mid /3$.

032719 'Constructing Elliptic Curves with Given Group Order over Large Finite Fields'
GJ Lay, HG Zimmer, *ANTS 94*

The authors describe a procedure for constructing elliptic curves with prescribed group orders over large finite fields. They consider two problems: given an integer $m > 3$, find a prime p and an elliptic curve over $GF(p)$ with order m; and given two integers n and $c_{\max}$, find an elliptic curve over $GF(2^n)$ with order cq, where q is prime and $c \leq c_{\max}$. The first is useful in primality proving, and the second in constructing elliptic curve cryptosystems.

032720 'Counting the Number of Points on Elliptic Curves over Finite Fields of Characteristic Greater than Three'
F Lehmann, M Maurer, V Müller, V Shoup, *ANTS 94*

The authors present a variant of Atkin's algorithm for counting the number of points on an elliptic curve over a finite prime field. The algorithm was tested on an example where p had 277 decimal digits: the time taken was about 572 MIPS days.

032721 'Straight-Line Complexity and Integer Factorization'
RJ Lipton, *ANTS 94*

The author shows that in a certain precise sense, if integer factorization is difficult, then the evaluation of polynomials with many rational roots is also difficult.

032722 'Factoring polynomials over finite fields using differential equations and normal bases'
H Niederreiter, *Mathematics of Computation v 62 no 206 (April 1994) pp 819 - 830*

The author extends his work with Göttfert (below) to demonstrate the usefulness of his polynomial factoring algorithm in large finite fields of small characteristic; the crucial linearisation step takes $O(d^e + (d^2 + d \log r)L(d))$ where d is the degree, $L(d) = \log d \log \log d$, $e < 2.4$ is the coefficient of fast matrix multiplication in the field, and r is the field's characteristic.

032723 'Factorisation of Polynomials over Finite Fields and Characteristic Sequences'
H Niederreiter, R Göttfert, *Journal of Symbolic Computation v 16 no 5 (Nov 93) pp 401 - 412*

The authors refine their techniques for factorising polynomials over finite fields using Hasse-Teichmüller derivatives, and in particular show that the linearisation step can be carried out in polynomial time for arbitrary finite fields.

032724 'Recurrent Sequences Modulo Prime Powers'
RGE Pinch, *Cirencester III pp 297 - 310*

The author presents a number of results about the period of linear recurrent sequences modulo a prime power. This can be complicated if the recurrence polynomial has repeated roots; the resulting ramification and its effects are discussed in some detail. The period can usually be determined uniquely from the polynomial.

032725 'Analysis of a Left-Shift Binary GCD Algorithm'
J Shallit, J Sorenson, *ANTS 94*

The authors present a new kind of left-shift binary algorithm for computing the greatest common divisor of two integers. They analyse its worst-case behaviour, and find that it uses about 27% fewer iterations than Euclid's algorithm for the worst-case input. Timings suggest that on average it is almost as fast as the usual binary algorithm, and for extended greatest common divisor computations it appears to be better.

032726 'Polylog Depth Circuits for Integer Factoring and Discrete Logarithms'
J Sorenson, *Information and Computation v 110 no 1 (April 94) pp 1 - 18*

The author studies parallel algorithms for factoring and discrete log. By working from the Dixon algorithm he shows that there is a probabilistic boolean circuit of size $\exp(O(n/\log^d n))$ and depth $O(\log^{2d+2} n)$ for factoring; the index calculus yields a similar circuit of the same size (but depth $O(\log^{2d+2} n + \log^3 n)$ for discrete log.

8 Theoretical Cryptology

032801 'Optimal Asymmetric Encryption'
M Bellare, P Rogaway, *Eurocrypt 94 pp 103 - 113*

From a trapdoor permutation f and an ideal hash function H, the authors construct a public key system in which an adversary can only create ciphertexts for which she already has the plaintext. It is thus secure against chosen ciphertext attack and is more efficient than the schemes of Damgård and Zheng/Seberry. The basic idea is that $E(x) = f(x \oplus G(r) \parallel r \oplus H(x \oplus G(r)))$, where r is a random number and G is a random function.

032802 'Dense probabilistic Encryption'
J Benaloh, *SAC 94 pp 120 - 128*

The author presents a probabilistic encryption technique based on factoring with the property that the ciphertext/plaintext ratio can be made arbitrarily close to unity, and discusses implications for secret sharing and balloting.

032803 'On the Dealer's Randomness required in Secret Sharing Schemes'
C Blundo, AG Gaggia, DR Stinson, *Eurocrypt 94 pp 37 - 47*

The authors prove upper and lower bounds on the amount of randomness required to set up a variety of secret sharing schemes. These bounds are tight in a number of cases, such as for small structures and odd cycles.

032804 'Linking Information Reconciliation and Privacy Amplification'
C Cachin, UM Maurer, *Eurocrypt 94 pp 269 - 278*

Both Maurer's noisy broadcast channel and quantum cryptography require a reconciliation step, in which the parties check their data and agree on an unconditionally secure key through some hashing or compression process. Privacy amplification, where the problem is to compress a partially secret string into a short, highly secret string, is a related problem, and the authors establish a general upper bound on the reduction of an opponent's collision entropy attributable to side information. With exponentially high probability, the eavesdropper obtains only 2(k + s) bits, where k is the number of check bits exchanged and s is a security parameter.

032805 'Parallel Divertibility of Proofs of Knowledge'
L Chen, IB Damgård, TP Pedersen, *Eurocrypt 94 pp 137 - 150*

The authors consider the limitations on diverting zero knowledge proofs, and show that two types of these cannot be diverted to two third parties simultaneously.

032806 'The size of a share must be large'
L Czirmaz, *Eurocrypt 94 pp 13 - 22*

The author extends previous results of Capocelli and others to show that for all n, there exists an access structure on n participants such that at least one of them must get a share which is $n/\log n$ times bigger than the secret. Furthermore, this is the best result which can be established using matroid and information theoretic techniques.

032807 'Parallel RAM algorithms for factorising words'
JW Daglein, CS Iliopoulos, WF Smyth, *Theoretical Computer Science v 127 no 1 (9/5/94) pp 53 - 67*

The authors show how to use $O(n/\log n)$ processors to factorise a Lyndon word of length n over an unbounded alphabet in $O(\log n \log\log n)$ time.

032808 'Orthogonal arrays and ordered threshold schemes'
E Dawson, ES Mahmoodian, A Rahilly, *Autralasian Journal of Combinatorics v 8 (Sep 93) pp 27 - 44*

The authors extend the results of Brickell and Davenport to show that if $M(t, w, v)$ is the maximum number of keys for an ordered perfect threshold scheme with threshold t, w participants and v shadows, then $M(t, w, v) \geq v$ with equality iff there exists an orthogonal array $(v^t, W+1, V, t)$. They also show that where $t = w$, such schemes can be constructed and implemented easily.

032809 'Round-optimal perfect zero-knowledge proofs'
G Di Crescenzo, G Persiano, *Information Processing Letters v 50 no 2 (22/4/94) pp 93 - 99*
The authors provide a 4 round (optimal) perfect zero-knowledge proof for membership of the set of quadratic residues, which uses a blob scheme based on factoring.

032810 'Identifying Randomness Given by High Descriptive Complexity'
WL Fouché, *Acta Applicanda Mathematicae v 34 no 3 (March 94) pp 313 - 328*
The author shows how algorithmic complexity can be used to find new proofs, and new versions, of results on random series and in combinatorics; in particular, every complex string can be viewed as a code of a universal graph, which can be randomly generated.

032811 'Blind Weak Signature and its Applications: Putting Non-cryptographic Secure Computation to Work'
M Franklin, M Yung, *Eurocrypt 94 pp 71 - 83*
The authors show how secure distributed computation protocols can be used to implement blind signatures that are checkable only by a third party; suggested applications include anonymous access control schemes, pseudonymous credentials and payment schemes.

032812 'A Taxonomy of Proof Systems (part 1)'
O Goldreich, *SIGACT News v 24 no 4 (Dec 93) pp 2 - 13*
This brief survey of proof systems covers interactive and noninteractive proofs, multiple provers, zero knowledge, probabilistically checkable proofs and knowledge extractors.

032813 'On Randomization in Sequential and Distributed Algorithms'
R Gupta, SA Smolka, S Bhaskar, *ACM Computing Surveys v 26 no 1 (March 94) pp 7 - 86*
The history of randomised algorithms goes back hundreds of years, and computer scientists have been increasingly interested in the subject since the 1970's. This extensive survey of the subject has a large annotated bibliography, and covers a number of areas of interest to cryptographers and computer security practitioners; these include primality testing, perfect hashing, zero knowledge, the dining philosophers' problem and Byzantine agreement.

032814 'On the Knowledge Complexity of Arthur-Merlin Games'
T Itoh, T Kakimoto, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 56–64*
In this paper, the authors investigate the knowledge complexity of interactive proof systems and show that (1) under the blackbox simulation, if a language L has a bounded move public coin interactive proof system with polynomially bounded knowledge complexity in the hint sense, then the language L itself has a one move interactive proof system, and (2) under the blackbox simulation, if a language L has a three move private coin interactive proof system with polynomially bounded knowledge complexity in the hint sense, then the language L itself has a one move interactive proof system. In addition, the authors show that there is a definite distinction between knowledge complexity in the hint sense and in the strict oracle sense.

032815 'On the Knowledge Tightness of Zero-Knowledge Proofs'
T Itoh, A Kawakubo, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 47–55*
In this paper, the knowledge tightness of zero-knowledge proofs is studied. The authors present a new measure for the knowledge tightness of zero-knowledge proofs, and show that (1) if a language L has a bounded round zero-knowledge proof with knowledge tightness $t(|x|) \leq 2 - |x|^{-c}$ for some $c > 0$, then $L \in \mathcal{BPP}$, (2) any language $L \in \mathcal{AM}$ has a bounded round zero-knowledge proof with knowledge tightness $t(|x|) \leq 2 - 2^{-O(|x|)}$ under the assumption that collision intractable hash functions exist, and (3) any language $L \in \mathcal{IP}$ has an unbounded round zero-knowledge proof with knowledge tightness $t(|x|) \leq 1.5$ under the assumption that non-uniformly secure probabilistic encryptions exist.

032816 'Checkers for Adaptive Programs'
T Itoh, M Takei, *SCIS 94 paper 6C*
The authors characterise the languages which have adaptive checkers, that is, a program to detect foreign code which adapts itself to behave like a member of the language. This provides an adaptive version of the work of Blum and Kannan.

032817 'Kolmogorov complexity Arguments in Combinatorics'
M Li, PMB Vitanyi, *Journal of Combinatorial Theory (series A) v 66 no 2 (May 94) pp 226 - 236*
The authors show that Kolmogorov complexity methods are useful in combinatorics by providing new proofs of a number of theorems on tournaments, coin weighing and the like. These proofs hinge of counting the bits in system descriptions and then observing a deficit somewhere.

032818 'An Anonymous Membership Proof System: Testable Invalidity of a User's Secret"
R Mizutani, T Matsumoto, *SCIS 94 paper 11D (in Japanese)*
Let us assume that information is distributed to allow individuals to prove that they are members of a predetermined group but without revealing the identities of the members. This paper shows what this information might comprise, and how to revoke or reinstate membership.

032819 'Simple Timing Channels'
IS Moskowitz, AR Miller, *Oakland 94 pp 56 - 64*
Shannon's definition of channel capacity as $C = lim_{n\to\infty} \frac{\log|S_n|}{n}$ (where the S_n are sequences) should actually be $C = limsup_{n\to\infty} \frac{\log|S_n|}{n}$, as the ordinary limit does not exist in many cases of practical interest, especially in the analysis of timing channels in multilevel secure systems. A new proof of the capacity bound is given based on the use of z-transforms; this reduces capacity bounds to radii of convergence, and can be used to determine the capacity of a number of complex timing channels. These typically turn out to be the roots of a real trinomial of the form $1 - x^{-a} - x^{-d}$ or $1 - x^{-a} - x^{-a-d}$, which can be found in closed form using special functions.

032820 'On Claw Free Families'
W Ogata, K Kurosawa, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 72–80*
This paper points out that there are two types of claw free families with respect to a level of claw freeness. The authors formulate them as weak claw free families and strong claw free families, and present the sufficient conditions for each type. A new example of strong claw free families is also given.

032821 'Authentication Codes in Plaintext and Chosen Content Attacks'
R Safavi-Naini, L Tombak, *Eurocrypt 94 pp 257 - 267*
Attacks on authentication codes may be classified according to the information available to the attacker: none (i.e., pure impersonation), ciphertext only (i.e., substitution), chosen ciphertext, plaintext, or chosen plaintext, or according to how success is defined: creating any valid message or correctly authenticating a chosen content. The authors use perpendicular arrays to transform plaintext attacks into attacks as difficult as pure impersonation, and than derive information theoretic bounds for the number of encoding rules needed to provide perfect protection against the two types of chosen content attack.

032822 'A Note on AM Languages Outside NP ∪ co-NP'
H Shizuya, T Itoh, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 65–71*
This paper investigated the AM languages which seem to be located outside NP ∪ co-NP. Two natural examples of such AM languages, the Graph Isomorphic Pattern (GIP) and the Graph Heterogeneity (GH), were given. The authors shown that the GIP is in Δ_2^P ∩ AM ∩ co-AM but is unlikely to be in NP ∪ co-NP, and that GH is in Δ_2^P ∩ AM but is unlikely to be in NP ∪ co-AM. They also shown that GIP is in SZK. Some structural properties related to those languages were also discussed.

032823 'Demonstrating Possession without Revealing Factors'
H Shizuya, K Koyama, T Itoh, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E77–A no 1 (1994), pp 39–46*

This paper presents a zero-knowledge interactive protocol that allows a prover to demonstrate that he really knows the two factors of a composite number without revealing the factors themselves. In this scheme, the factors need not be primes. The security of the protocol is based on the difficulty of computing discrete logarithms modulo a large prime.

032824 'Combinatorial Techniques for Universal Hashing'
DR Stinson, *Journal of Computer and Systems Sciences v 48 no 7 (April 94) pp 337 - 346*

The author characterises Carter and Wegmann's universal hash functions in terms of balanced incomplete block designs and orthogonal arrays. He shows that these two approaches lead to slightly different natural definitions; and, conversely, design theory can be used to give new constructions of hash functions.

032825 'Decomposition Constructions for Secret-Sharing Schemes'
DR Stinson, *IEEE Transactions in Information Theory v 40 no 1 (Jan 94) pp 118 - 125*

Every graph of maximum degree d has a perfect secret-sharing scheme with information rate $2/(d+1)$; it follows that the maximum rate of such schemes for paths on more than 3 vertices and for cycles on more than 4 vertices is 3. The article also describes a linear programming approach, and provides a number of worked examples.

032826 'Near Optimal Unconditionally Secure Authentication'
R Taylor, *Eurocrypt 94 pp 245 - 255*

The author has constructed a new arbitrated authentication code, which is efficient with respect to key sizes, codeword lengths, and computation time. It is unconditionally secure, and the arbiter cannot impersonate the sender. It is based on a geometric construction, which is an optimised modification of the one presented by Desmedt and Yung at Crypto'90. An optimised, unarbitrated Wegman-and-Carter based scheme is also given.

032827 'A Linear Construction of Perfect Secret Sharing Schemes'
M van Dijk, *Eurocrypt 94 pp 23 - 26*

The author gives an algorithm which, given any rational number, can decide whether there exists a perfect secret sharing scheme with this rate and, if so, construct an example using matrices. The information rate of a scheme constructed in this way is equal to that of its dual; and there are relationships with linear codes and with previous constructions.

032828 'Coding Theorems for Shannon's Cipher System with Correlated Source Outputs and Common Information'
H Yamamoto, *IEEE Transactions on Information Theory v 40 no 1 (Jan 94) pp 142 - 144*

The author examines the admissible key rate in a system where plaintext words are correlated with each other, and shows that where X and Y are correlated, $I(X,Y)$ and $min\{H(X),H(Y)\}$ give maxima and minima for the saving in keystream. He also discusses complications, such as if only one of X and Y is secret.

9 Book Reviews

'METEOR BURST COMMUNICATIONS: THEORY AND PRACTICE'
DL Schilling (editor)
Wiley 1993, ISBN 0-471-52212-0

The ionised trails of micrometeors entering the earth's atmosphere reflect radio waves, especially in the low VHF band, and attempts have been made since the 1960's to use this phenomenon for communication. Although the initial interest in the subject faded with the introduction of satellites for the bulk of beyond-line-of-sight communications, meteor burst communications are now used in a number of military and intelligence rôles. Their intermittent nature, and the relatively small ground footprint of each trail, make them inherently hard to monitor.

This book is the first comprehensive guide to the subject to appear in modern times. Such a guide is welcome, as the subject spans a very wide range of subject matter: from the physics of the meteor trails themselves through the various coding and other techniques which are used to maximise the available channel capacity through to a number of issues arising from practical engineering experience.

The core of the book of a long chapter by Robert Desourdis which works through from physical data, such as the arrival rates of micrometeors at various times and latitudes, to provide a systematic guide to engineering parameters such as wavelengths, duty cycles and power budgets. Further chapters look at advanced techniques such as the use of adaptive data rates and coding schemes, the channel capacity and how this can be approached by various modulation schemes.

The context of the book is a US Air Force network in Alaska, which provides backup communications for early warning radars in the event that satellite communications are knocked out. Most of the authors appear to have worked on this system.

'SECURITY ARCHITECTURE FOR OPEN DISTRIBUTED SYSTEMS'
S Muftic, A Patel, P Saunders, R Colon, J Heijnsdijk, U Pulkinnen
Wiley 1993, ISBN 0-471-93472-0

This book presents a survey of existing open system security mechanisms, and proposes a coherent superset called the Comprehensive Integrated Security System (CISS). It is based on an EC project which ran from 1985 to 1990, and has an email flavour; it goes into the mechanisms of X.400 and X.500 in detail and draws on the OSI security model.

CISS provides a wide range of services; in addition to the usual secrecy, integrity and key management functions, it tackles anonymous communications, contract signing, threshold schemes, copyright licensing, notarisation, logging and security recovery. Not all these features are developed at the same level of detail, but the book gives a vision of how open system security might develop.

At the level of mechanisms, CISS assumes one security management centre per domain, plus a library of cryptographic and access control functions to be made available to users and applications. The management centre consists of a security database, plus a number of agents controlling access to mechanisms and the various communications, monitoring and recovery functions.

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.

Subscription rates: Regular subscriptions cost £95, and individual subscriptions are available at the reduced rate of £60. Purchase orders are accepted for regular 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 1994 subscription plus a complete set of 1992 and 1993 back numbers at a price of £90 for individual subscribers and £145 for regular subscribers. This back number offer is only available while stocks last.

Individual subscription for v 3 (1994) - Please debit my VISA/MasterCard with £60 ☐ I enclose a cheque for £60 ☐ / US$90 ☐

Individual subscription for all issues to end 1994 (v 1, 2 and 3) - Please debit my VISA/MasterCard with £90 ☐ I enclose a cheque for £90 ☐ / US$135 ☐

Regular subscription for v 3 (1994) - Please debit my VISA/MasterCard with £95 ☐ I enclose a purchase order ☐ / cheque ☐ for £95 ☐ / US$142.50 ☐

Regular subscription for all issues to end 1994 (v 1, 2 and 3) - 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, Cambridge CB5 9HF, UK