Computer and Communications

Security Reviews

Volume 2 Number 1 March 1993

CONTENTS

This journal reviews research in computer and communications security. Work published in major journals and conferences will be 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

Welcome to the second edition of 'Computer and Communications Security Reviews'. In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by 9 February 1992; and books and technical reports received by the editor prior to this date.

We also have reviews of a few papers from Eurocrypt 92 and Crypto 92 which were not ready in time for the previous issue; and reviews of papers presented at the following conferences:

Workshop on Foundations of Computer Security, 16-18/6/92, Franconia, USA ('Franconia') *ISBN: 0-8186-2850-2*
Chinacrypt 92, 18-21/8/92, Guiyang, Guizhou, China, *(ISBN 7-03-003069-9/TP-224)*
IFIP 1992 Congress, 'Education and Society', 7-11/9/92, Madrid, Spain *Proceedings: IFIP A-13 vol II, North-Holland (ISBN 0926-5473)*
15th National Computer Security Conference, 13-16/10/1992, Maryland, USA, *National Institute of Standards & Technology (US GPO:1992-625-512:60546)*
ESORICS 92 (European Symposium for Research in Computer Security), 23-25/11/92, Toulouse, France *Springer Lecture Notes in Computer Science vol 648 (ISBN 3-540-56246)*
Auscrypt 92, 13-16/12/92, Gold Coast, Queensland, Australia *Proceedings to be published in Springer Lecture Notes in Computer Science series*

Subscription and 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 CB5 9HF
United Kingdom

Corporate subscriptions: These are £95 or $145: send your cheque or purchase order to the publishers at the above address.

Individual subscriptions are available at the reduced rate of £60 or $95: send a cheque (sorry, no purchase orders!) or subscribe by credit card. Both VISA and MasterCard are accepted and charged at £60. We need a letter with your name, cardholder address, delivery address (if different), card account number, expiry date, and signature; this letter can be sent by post or faxed to Cambridge (+44 223) 334678.

1 Applications and Engineering

021101 'Marking the cards'
D Austin, *Banking Technology, Jan 92, pp 18 - 21*

Credit card fraud losses in the UK were stable at 0.13% of turnover until 1989, but increased to 0.25% in 1990 and are still rising. 30% of these losses are due to postal interception. Sharing information on 'risky' names and addresses is estimated to have saved £10m. The article also discusses other security measures, such as whether cards should carry photographs.

021102 'Card Fraud: Banking's Boom Sector'
Banking Automation Bulletin for Europe, Mar 92, pp 1 - 5

Card counterfeiting is relatively easy, but it took organised crime two decades to realise this. Once they did, in the mid-80's, losses started to increase geometrically. Loss statistics are presented for a number of countries, and the fraud control strategies of banks in Spain, France and the UK are discussed. Spain has been the most successful: their introduction of online-only eftpos has reduced losses from 0.21% of turnover in 1988 to 0.008% in 1991.

021103 'Special Report - Security'
Banking World v 10 no 1 (92) pp 27 - 31

The use of photographs on payment cards is likely to have little effect on fraud unless retailers have to pay for transactions on stolen cards, but this is not allowed by the major operators' worldwide terms of trade. Smartcards are currently justified for corporate payments, and are also used in an EDI demonstrator project in the UK.

021104 'Special Report - Electronic Funds Transfer at the Point of Sale'
Banking World v 10 no 6 (92) pp 27 - 32

This article describes STASIS, a system which allows smaller UK financial institutions to get access to the 'Switch' debit card system. It also discusses fraud in EFT: although the use of PINs and biometrics at the point of sale is often advocated, lowering the floor limit is the technique most used in practice. The main application of smartcards in EFT in Britain is as secure transaction memory for retailer terminals.

021105 'Special Report - Annual Review of Electronic Banking and Technology'
Banking World v 10 no 11 (92) pp 26 - 39

This survey presents ATM statistics, including machine types installed, for UK banks and building societies. It lists the facilities offered by individual institutions and the networking arrangements between them. It also surveys BACS, PC-based banking systems and signature verification technology.

021106 'Precise Identification of Computer Viruses'
LE Bassham III, WT Polk, *Proc 15th NCSC p 494 - 502*

Computer viruses can have many variations, which can be as simple as a print string or the means to clear a register. Classifying them properly is important, as variations of the same virus can usually be removed in the same manner. Further research is proposed to unify and standardize the maps and other methods used to identify the various types of viruses.

021107 'A quantum leap in secret communications'
W Bown, *New Scientist no 1858 (30 Jan 1993) p 21*

British Telecom's research laboratories announce that they succeeded in sending a message encrypted using quantum cryptography over a distance of ten kilometres. This indicates that it may be possible to build working cryptosystems based on this technology.

021108 'GDoM - a multilevel document manager'
C Calas, *Proc. ESORICS 92, pp 393 - 408*

This is an application which uses M^2S, the secure Unix processor described below, to provide multilevel security for a document library. The librarian, which controls access and maintains coherence, invokes the M^2S hardware security subsystem directly to validate requests. This project illustrates how hardware controls can help enforce application security in such a way that only the application's interfaces need be trusted.

021109 'Fine-Grained Access Control in a Transactional Object-Oriented System'
LF Cabrera, AW Lumiwski, JW Stamos, *Computing Systems v 5 no 5 (92) pp 199 - 216*

The access control component of the IBM Melampus project is described. This checks every method invocation using access control lists. Data structures are discussed; a current principal is associated with each thread and reuse ensures that the number of access control lists is very much less than the number of objects. As a simple query can interrogate arbitrarily many objects and run indefinitely, revocation is given priority at the expense of serialisability.

021110 'Implementation of Security Functions into File Transfer Access and Management Protocol'
H Chang, O Monkevitch, WA McCrum, *IFIP 92 pp 547 - 553*

The authors point out the vulnerability of passwords in the ISO/IEC 8571 FTAM protocol to interception at lower OSI layers, and report a security enhancement in which passwords are encrypted using a secret key and a timestamp which is valid for only a few minutes. Various system implications are discussed.

021111 'Repelling the Hack Attack'
M Cheek, A Steffora, *Computer Weekly, Jan 28 1993 p 31*

Last year, hackers discovered how to break into Novell Netware files and applications. A quick fix was produced, but the long term strategy involves two phases: in the first, available last October, network protocol data are encrypted, and in the second, software enhancements will be available which allow user data to be encrypted as well. However, earlier versions of Netware are still vulnerable.

021112 'Defense-in-Depth Against Computer Viruses'
FB Cohen, *Computers and Security vol 11 no 6 (Oct 1992) pp 563 - 579*

Viruses have demonstrated that integrity is an aspect of computer security which was neglected until recently. An overview is given of viruses and of the common countermeasures such as scanners, self-testing programs and vaccination. Smarter viruses get round some of these, so that one really has to use cryptographic checksums rather than CRCs. Real virus protection must depend on a close analysis of the boot process, and a variety of techniques used to protect attacks on each phase of this. This is implemented in the ASP toolkit.

021113 'M^2S - A Machine for Multilevel Security'
B d'Ausbourg, JH Llareus, *Proc. ESORICS 92, pp 373 - 391*

A computer is described which implements information flow control in hardware. This is achieved using a security subsystem which controls the level of objects each process can observe. As a result, the operating system does not need a trusted kernel, but does need to anticipate the hardware controls when multiplexing tasks and handling multilevel files. Such hardware control gives strong security for relatively few components.

021114 'Breaking the Traditional Computer Security Research Barriers'
Y Desmedt, *Proc. ESORICS 92, pp 125 - 138*

This article presents an overview of research in computer and communications security, covering identification, covert channels, threshold schemes and reliability. It argues that future trends will continue to be away from multiuser systems and toward single-user machines, particularly notebooks. In this case, much more secure systems can be built, and cryptology will be the key enabling technology.

021115 'Electronic payment systems'

J Essinger, *Financial Technology Insight (part 1:) April 92 pp 11 - 15 (part 2:) May 92 p 13*

Statistics are provided of ATMs, eftpos and telephone banking in the UK, USA, Belgium, France, Germany, Holland and Portugal.

021116 'The Need for a Multilevel Secure (MLS) Trusted User Interface'

G Factor, S Heffern, D Nelson, J Studt, M Yelton, *Proc 15th NCSC pp 423 - 428*

Trusted multilevel user interfaces are needed which allow users to display information of multiple classifications on a screen at once. Such an interface should allow the user to obtain the label of data on a screen in a trustworthy (not advisory) fashion and prevent high level data from being entered into a low level field. The authors claim that such an interface should be easy to build at the TCSEC B3 level.

021117 'Trusted Third Parties'

Financial Technology Insight, August 92, pp 18-19

This article describes the service offered by Veridial, a French electronic notary service, which is owned by France Telecom and a consortium of banks. Its clients use DES to generate digital signatures on transactions using smartcards; these are verified by the notary and signed again using RSA so that they can be checked by any recipient. Transactions are also archived on write-once optical disk in case of dispute.

021118 'Special report - Eastern Europe'

Financial Technology International Bulletin v 9 no 10 (6/92)

ATM networking was the key technology in promoting banking systems development in Spain and Portugal in the early 1980's, as rapidly increased machine availability fostered takeup of bank accounts by the population. The same could be done in Eastern Europe and should be a priority; it is argued that EC and other development aid should be made available to transfer the necessary know-how.

021119 'Special report - payment card security'

Financial Technology International Bulletin v 9 no 11 (7/92)

This article reports two systems under development by the British Technology Group - one checks vein patterns in the subject's left hand, and the other is a signature verifier which tracks pen movement in the air as well as on the tablet.

021120 'A Practical Analog Voice Scrambling System'

YL Gao, CR Zhong, *Proc. Chinacrypt 92 pp 34 - 39*

This paper presents and discusses an analogue voice scrambler which operates in three dimensions (amplitude, frequency and phase) under microcomputer control. It has high security, low cost and good voice quality.

021121 'DASS: Distributed Authentication Security Service'

M Gasser, C Kaufmann, J Linn, Y le Roux, J Tardo, *IFIP 92 pp 447 - 456*

This article describes DEC's security product, DASS, which has been proposed as an Internet Standard and provides the authentication service part of DSSA, the DEC security architecture. It makes extensive use of RSA to provide mutual authentication, privacy and signature functions. Global identity and network login are supported, as are multiple certification authorities, and timestamps are used rather than challenge-response. The authentication mechanism is described in some detail.

021122 'Experience with a Penetration Analysis Method and Tool'
S Gupta, V Gligor, *Proc 15th NCSC pp 165 - 183*

Penetration analysis has traditionally been done in an ad hoc manner. A tool is described here which partially automates finding flaws in source code, and several examples are presented of flaws which could be used to penetrate Secure XENIX. The tool works by generating the set of all execution paths, and evaluating a number of penetration resistance principles (such as consistent validation and lack of dependencies) along each of them.

021123 'Application Layer Security Requirements of a Medical Information System'
D Hamilton, *Proc 15th NCSC pp 9 - 17*

This paper surveys security requirements for medical information systems. These are similar to military needs, but the priorities are very different. In particular, medical systems must have methods to override access controls in emergency situations. In these cases, detailed auditing is the key to accountability. Furthermore, access controls are based on roles, rather than simple user identity. Other crucial areas for medical systems include data integrity and authentication (of both system users and patients).

021124 'Electronic Purses'
P Harrop, *Banking Technology, Dec 91/Jan 92, pp 26 - 28*

This article discusses the business and technological issues raised by prepayment tokens such as phone cards and transport tickets. Universal cards, which can be used to pay for several services, have been introduced in Japan, Denmark and the USA. Magnetic and optical cards predominate, especially in transport, but memory chip cards are slowly taking market share.

021125 'A Unix Network Protocol Security Study: Network Information Service'
DK Hess, DR Safford, HW Pooch, *Computer Communication Review v 22 no 5 pp 24 - 28*

This article reports penetration experiments against Sun Microsystems' NIS, in which an intruder using a lightly loaded machine was consistently able to beat the server and forge RPC messages. Various possible modifications are discussed.

021126 'Piloting authentication and security services with OSI applications for RTD information (PASSWORD)'
PT Kirsten, P Williams, *Computer Networks and ISDN Systems v 25 (92) pp 483 - 489*
This paper describes a current EC project to demonstrate that security enhanced X.400 and X.500 services can be operated without hampering these systems' openness and usability. It uses MD2, MD4 and RSA to provide the first large-scale certified directory, and will examine various practical aspects of such security services.

021127 'Concept for a Smart Card Kerberos'
M Krajewski, *Proc 15th NCSC pp 76 - 83*

Kerberos is increasing in popularity for distributed authentication in workstation networks. However, the user may be compromised when entering his password. It is therefore suggested that critical portions be moved into a smart card; this could be done in a way invisible to the Kerberos server and thus allow phased implementation.

021128 'Where cash is king'
D Lane, *Banking Technology, Oct 92, pp 38 - 41*

This article describes the state of electronic banking systems in Italy. Cheques currently take 11 days to clear, but it is hoped that truncation will reduce this to 5 days. Meantime the use of cash is widespread and ATM use is increasing, although losses are some 0.5%. This is attributed to offline operation and should decrease next year when ATMs go online. False ATMs, which capture customer card and PIN data, have been a problem.

021129 'Automated Audit Trail Analysis for Intrusion Detection'
T Lunt, *Computer Audit Update, April 1992, p 2 - 8*

This article describes SRI's IDES project, which uses an expert system running on Sun hardware to examine audit trails from a variety of machines. The analysis can be online or offline, and tries to find both internal and external attacks by looking for departures from normal patterns of activity. Different approaches can be used at different levels of the system being monitored.

021130 'Extending Our Hardware Base: A Worked Example'
N McAuliffe, *Proc 15th NCSC pp 184 - 193*

This paper describes how TIS went about extending the B2 rating of Trusted XENIX from the IBM PC-AT and PS2 platforms to six PC clones. The necessary changes were examined to see if they affected the TCB interface, and if so given additional scrutiny. A series of analyses and reports were developed to describe the hardware differences, and to verify that covert channels were not introduced. A limited penetration effort was also performed.

021131 'KryptoKnight Authentication and Key Distribution System'
R Molva, G Tsudik, E van Herreweghen, S Zatti, *Proc ESORICS 92, pp 155 - 174*

This paper describes an authentication and key distribution system which has been developed by IBM for Unix based systems and which supports the relevant IBM application programming interfaces. Based on Kerberos, it uses secret key cryptography and an authentication server, but allows either the initiator or recipient of a secure session setup to interface with this server. The cryptography may not only be based on DES, but also on hash functions such as MD5 in the hope that this will facilitate exports.

021132 'Implementation of the Comprehensive Integrated Security System for computer networks'
S Muftic, *Computer Networks and ISDN Systems v 25 (92) pp 469 - 475*

This paper describes CISS, which provides a library of encryption and security functions, a DES/RSA based file transfer protocol, and operating system level security for PCs and mainframes.

021133 'CISS: Generalised Security Libraries'
S Muftic, E Hatunic, *Computers and Security v 11 no 7 (11/92) p 653 - 659*

This describes two publicly available 'C' libraries: one implements various encryption algorithms and related functions such as primality testing, while the other incorporates these in various security routines. It also describes the implementation and testing of these libraries.

021134 'New Protocols for Electronic Money'
JC Pailles, *Proc Auscrypt 92,*

This article reviews various digital cash protocols and proposes new versions based on the Guillou-Quisquater and Schnorr signature schemes.

021135 'Security Constraint Processing in Multilevel Secure AMAC Schemata'
G Pernul, *Proc ESORICS 92, pp 349 - 370*

The AMAC design environment assists designers of secure database systems in classifying data. This is done at the design phase, as security checking at runtime is expensive. Protection is offered at the fragment level, and the fragments arise from a structured decomposition of a database diagram. Fragment dominance relationships are then used to derive security labels, which are implemented using database triggers.

021136 'Architectural Implications of Covert Channels'
N Proctor, P Neumann, *Proc 15th NCSC pp 28 - 43*
This paper reviews covert channels: how they occur, what assumptions are needed to ignore them, how to eliminate them from resource allocation algorithms and what the tradeoffs are. It then proposes an architecture for eliminating them and describes a design for a multi-level disk drive

using manual allocation. This drive can allow read-down and write-up operations which have no covert channel but still yield adequate performance. The authors argue that building secure operating systems is beyond today's technology, and argue that using single-level processors with a multi-level disk gives maximum assurance at a reasonable cost.

021137 'COSINE Sub-Project P8: security services'
M Purser, *Computer Networks and ISDN Systems v 25 (92) pp 476 - 482*

This paper describes a current EC project to demonstrate that secure email and secure remote access can be provided quickly using public key routines and a certification authority.

021138 'Checksumming Techniques for Anti-Viral Purposes'
Y Radai, *Proc IFIP 92 pp 511 - 517*

This paper describes the use of checksumming techniques to prevent any file modification going undetected. Such techniques must be implemented with due regard to the characteristics of the local operating system: for example, many products would check the integrity of a file FOO.EXE but not check whether a virus had introduced an extra file FOO.COM, to which DOS would give preference. Furthermore, such checksumming techniques are harder to circumvent if they are dependent on a cryptographic key.

021139 'A Modular Exponentiation Unit based on Systolic Arrays'
J Sauerbrey, *Proc Auscrypt 92,*

This article describes the design of a modular exponentiation unit constructed from two systolic arrays, which perform multiplication and Montgomery reduction simultaneously. It improves upon previous designs by handling multiple bits of the operands at the same time. A data rate of 215Kbit/sec is projected for 512-bit RSA.

021140 'Software Forensics: Can We Track Code to its Authors?'
EH Spafford, SA Weeber, *Proc 15th NCSC p 641 - 650*

Handwriting analysis can be used to determine who wrote a document. In a similar fashion software forensics should be able to track software back to its creator, based on individual programming styles. Source code may contain stylistic evidence including source language, formatting style, commenting style, variable naming, spelling errors, and use of language features. Even binary code retains evidence of its author's style, including use of data structures, algorithms, level of programming skill, and errors in the code. Although there seems to be plenty of data, at this time there is still no way to use it to match code to an author.

021141 'Feasibility Study of Adding Security Facilities to the DECnet VAX Network'
ZL Song, GQ Ni, *Proc. Chinacrypt 92 pp 247 - 252*

The implementation of the DECnet VAX data link layer are analysed and some schemes for adding security to this layer are proposed. Their feasibility is studied and various system design issues are discussed.

021142 'Associating metrics to Certification Paths'
A Tarah, C Huitema, *Proc ESORICS 92, pp 175 - 189*

The Chimaera security model developed by INRIA has been extended to cover certification paths. These are chains of cross-certificates issued by certification authorities intermediate between two subjects who wish to communicate. As it may not always be wise to place complete trust in all authorities, mechanisms are presented for dealing with partial trust and multiple paths.

021143 'Policy Enforcement in Stub Autonomous Domains'
G Tsudik, *Proc ESORICS 92, pp 229 - 257*

This paper presents the latest version of the 'visa' protocol, whose function is to enforce access control between autonomous domains of a network. Each domain's access control server grants visas to hosts in its jurisdiction which want to communicate with foreign hosts; these visas are included in message packets and checked by the gateway. The new version uses timestamps or packet counts to prevent certain replay attacks, and the system implications of this are discussed.

021144 'Retailers evade the Eftpos net'
S Turner, *Banking Technology, May 92, pp 20 - 23*

In Germany, the banks have created an infrastructure for PIN-based eftpos, but this is so expensive (at about 1% of turnover) that only 2,000 of the country's half million retailers have signed up. The store chain Peek & Cloppenburg is developing an alternative signature-based system, but the banks will not guarantee payments on this. The compromise is likely to be a hybrid system, which will let retailers start with signatures and upgrade to PINs later.

021145 'The Development and Testing of the Identity-Based Conference Key Distribution System for the RHODOS Distributed System'
M Wang, A Goscinski, *Proc. ESORICS 92, pp 209 - 228*

This paper describes the implementation of cryptographic functions in a distributed operating system. The system has a central key server, plus an agent in each node which enforces what users can do. The algorithm which was used was broken while the system was being developed; but as the designers gave users no access to their secret keys, and the attack relies on users conspiring to share their secret keys, it is claimed to have a limited effect on the system security.

021146 'Is there anyone out there?
M Whybrow, *Banking Technology May 1992 pp 38 - 40*

Voice recognition technology has been introduced at a number of banks. However the experience of five banks surveyed - three UK, one Irish and one Finnish - is that customer reaction to these systems has been overwhelmingly negative.

021147 'The storm before the calm'
M Whybrow, *Banking Technology Oct 1992 pp 18 - 22*

EDI systems face a number of legal problems, such as the admissibility of computer records in evidence. Most equipment vendors are just pushing on regardless and hoping for a reasonable outcome. There are also technical problems, especially with linking EDI to payment systems, which few firms do yet. SWIFT's EDI service is briefly described.

021148 'A Tool for Covert Storage Channel Analysis of the UNIX Kernel'
DA Willcox, SR Bunch, *Proc 15th NCSC pp 697 - 706*
The authors describe a tool developed at Motorola to perform a covert storage channel analysis on annotated C source code.It was used to analyse UNIX system source code targeted at a B2 evaluation. As it is automated, it can be used more easily than a shared resource matrix; it reports potential covert channels for manual review. Sixty-five potential covert channels were found in one operating system implementation: they are divided into shared identifiers, resource exhaustion, caches, and direct covert channels, and several of them are discussed.

021149 'A new analogue speech scrambling scheme'
BN Yang, HL Zheng, YM Wang, *Journal of Xidian University v 19 no 1 (92) pp 25 - 29*

A new analogue speech scrambler is proposed, which uses a discrete cosine transform with dummy spectrum insertion. Its security and reliability are analysed; a weighting function is presented for selecting permutations, and some computer simulation results are given.

021150 'Attribute Support for Inter-Domain Use'
ME Zurko, *Proc Franconia 92 pp 179 - 188*

The author describes a tool called UAS (User Attribute Service) whose function is to maintain security related information on behalf of users of a large distributed system. She considers the case of multiple security domains and contrasts local and remote control of attributes. The design included careful consideration of the ergonomics of the system in addition to its security.

2 Operating System and Database Security

021201 'Secure Dependencies and Dynamic Level Assignments'
P Bieber, F Cuppens, *Proc Franconia 92 pp 63 - 75*

The authors examine dynamic security levels in a multi-level secure system. Their example is a secret level user who wishes to perform an unclassified job. They suggest that 'tranquillity' (including static level assignment) is necessary for certain security policies, and examine some consequences of relaxing this constraint.

021202 'Towards Security in an Open Systems Federation'
JA Bull, L Gong, KR Sollins, *Proc. ESORICS 92, pp 3 - 20*

Open systems will have no common security infrastructure, and so the current emphasis on administrator imposed security policies will have to change. Ultimately, the capability to access an object will have to be controlled by the object itself. Chains of service are always cyclic, and, in the absence of a central access control node, a security policy may be enforced using access certificates and security servers. The protocols necessary to achieve this will combine authentication and delegation.

021203 'Enforcing Entity and Referential Integrity in Multilevel Secure Databases'
VM Doshi, S Jajodia, *Proc 15th NCSC pp 134 - 143*

Enforcing referential integrity in multi-level relational databases is complex, because insertion, deletion, and update can cause information flows and allow inference. Referential integrity rules are proposed which depend on whether the foreign key is at a higher, equal or lower classification than the primary key, and can be set up with or without polyinstantiation. Examples are presented to justify the rules, and a table is provided which shows the allowed and unallowed actions for element, tuple (row), attribute (column), and relation level labeling.

021204 'An Object-Oriented View of Fragmented Data Processing for Fault and Intrusion Tolerance in Distributed Systems'
JC Fabre, B Randell, *Proc. ESORICS 92, pp 193 - 208*

In many applications, the sensitivity of the data in an object is contained in the links between objects. For example, in a payroll file, it is the relationship between names and salaries which must be kept confidential. We can use a security server to fragment such objects, and then process the fragments on an unclassified distributed network. To illustrate this idea in greater detail, a distributed diary was implemented as an ESPRIT research project.

021205 'A Foundation for Covert Channel Analysis'
T Fine, *Proc 15th NCSC pp 204 - 212*

This paper describes two methods of analyzing covert channels: using information flow tools (referred to as ft-policy) and using non-interference analysis (referred to as ni-policy). Comparing them shows that some systems can be secure with respect to ni-policy but not with respect to ft-policy, because of weaknesses in the ft-policy's definition of covert channels. However, any system which is secure with respect to the ft-policy is also secure with respect to the ni-policy. Surprisingly, this does not imply that the ni-policy is weaker. Rather, it shows that the ni-policy avoids certain 'false positives' which the ft-policy uncovers.

021206 'Aggregation and separation as noninterference properties'
SN Foley, *Journal of Computer Security v 1 no 2 (1992) pp 158 - 188*

Some information flow policies may have exceptions, which might result from separation-of-duty requirements or aggregation policies. The latter include the status of derived information (anything derived from confidential and top secret information must, for example, be classified top secret), and Chinese Wall policies (a consultant can read information on bank A or bank B, but not both). A formal framework for the classification of flow policies is presented, and noninterference is defined in terms of sequences of actions and views. The set of information which may flow to a given user is examined, unwinding lemmas are proved, and these unwinding conditions are shown to be sufficient.

021207 'Separation Machines'
J Graff, *Proc 15th NCSC pp 631 - 640*

A separation machine partitions a computer into several domains, each of which can run a separate operating system, and thus provides an isolation security policy. Some of the domains could be trusted and some untrusted, and could even implement different security policies, but the overall system would retain a high level of assurance.

021208 'Operating System Support for Trusted Applications'
R Graubert, *Proc 15th NCSC pp 459 - 466*

Trusted applications such as multi-level secure DBMSs are often needed to extend operating system security (e.g., by adding integrity policies to existing confidentiality policies) or to provide finer grained control on objects. To minimize the impact of trusted applications on underlying trusted operating systems, features such as extensible trusted path facilities, fine grained privileges, privilege bracketing, application encapsulation, and fine grained (byte level) data labeling are needed.

021209 'Towards a theory of penetration-resistant systems and its applications'
S Gupta, VD Gligor, *Journal of Computer Security v 1 no 2 (1992) pp 133 - 158*

Previously, penetration testing of systems consisted of amassing a number of hypotheses about possible flaws, which would then be tested. The authors try to sytematise this, and argue that most penetrations arise either from parameter validation errors or from timing errors. They conclude that penetration resistance should be built in at the system call level, and that it must provide a number of features, specifically isolation, noncircumventability, consistency of global system variables, timing consistency, and the elimination of undesirable dependencies. These properties are reduced to checking and invariance conditions, and a flow-based formal model for verifying these conditions is outlined.

021210 'Reducing the Proliferation of Passwords in Distributed Systems'
RC Hauser, ES Lee, *IFIP 92 pp 525 - 531*

The proliferation of passwords has become a problem, and if users have too many passwords, then they will use weak ones or write some of them down. It is proposed instead that there should be only one logon, to the local workstation, which should then in turn log on to remote hosts using machine generated passwords. This can be further strengthened by encryption.

021211 'Measuring the Effect of Commutative Transactions on Distributed Database Performance'
S Jajodia, R Mukkamala, *Information Sciences v 68 (1993) pp 91 - 111*

Commutative transactions are those which can be carried out in any order, and they can be used to reduce the number of cyclic and dependency conflicts which occur when updating a partitioned distributed database. A model is developed to estimate the effect of this.

021212 'Secure Open Systems'
P Kaijser, *Computer Fraud and Security Bulletin Nov 92 pp 12 - 18*

COMPOSITE is an EC project to study various available security architectures. The article presents a survey of three of these, namely DSSA, OSF DCE and SESAME, and compares their features.

021213 'On Transaction Processing for Multilevel Secure Replicated Databases'
IE Kang, TF Keefe, *Proc. ESORICS 92, pp 329 - 347*

This paper discusses the problems of transaction scheduling protocols in multilevel systems.

In particular, a multilevel replicated architecture has one database for each security level, plus a transaction manager which writes transactions to them from the lowest applicable security level upwards. Previous protocols for this are shown to suffer from a problem, in that a covert channel can arise between databases at incomparable security levels; this may be prevented by controlling the commit order as well as the submission order of transactions.

021214 'A Nonce-based Protocol For Multiple Authentications'
A Kehne, J Schönwalder, H Langendörfer, *Operating Systems Review v 26 no 4 (Oct 92) pp 84 - 89*

A protocol is presented which is inspired by Kerberos but does not require synchronised clocks. Instead, it uses nonces to generate a session key and a ticket, which can be used for repeated authentications during a predetermined period. The protocol's correctness is demonstrated using the BAN logic.

021215 'Type-level Access Controls for Distributed Structurally Object-Oriented Database Systems'
U Kelter, *Proc. ESORICS 92, pp 21 - 40*

Distributed object-oriented databases present some hard access control problems. For example, the objects of a CASE tool might be program modules containing source code, review results, completion deadlines and accounting information, which all have different access profiles. It is suggested that object management systems should implement access rules along with the type definitions. Furthermore, a simple hierarchy is insufficient because of need for separation of duties and the conflicts which arise from this (such as between the author and reviewer of source code). For this reason, the use of three-valued logic is proposed, in which access variables take the values (yes, maybe, no), and an experimental implementation is described.

021216 'On the Chinese Wall Model'
V Kessler, *Proc. ESORICS 92, pp 41 - 54*

The Brewer-Nash 'Chinese Wall' model of computer security turns out to have an undesirable consequence: a subject can write only when he has read access to at most one object. Once he acquires read access to a second object, he cannot write at all. A way out is suggested, in which conflict-of-interest relations are stored in a matrix and upgraded every time a new write access is granted.

021217 'Implications of Monoinstantiation in a Normally Polyinstantiated Multilevel Secure Database'
FE Kramer, SM Heffern, *Proc 15th NCSC pp 236 - 242*

An MLS database application is described where polyinstantiation is used for cover stories. For a 'remarks' relation in the database, low data may be replaced by high data, causing the destruction of the low data. There may be multiple 'remarks' for a given record, each identified by a chronological sequence. The uses and security impacts of this architecture are explained.

021218 'On the design and administration of secure database transactions'
EV Krishnamurthy, A McGuffin, *ACM SIGSAC Review v 10 pp 63 - 70*

This article describes how user security constraints can be built into database systems. Business rules can be implemented as integrity checks, which might for example perform incremental audit operations when balances are updated. The programming of user profiles is also discussed.

021219 'Timely Authentication in Distributed Systems'
KY Lam, T Beth, *Proc. ESORICS 92, pp 293 - 303*

In general, timestamps give the most appropriate freshness assurance for packet switched communications, while challenge-response protocols are better in circuit switched environments. The latter involve protocols which establish state information, which the former do not always do this; and challenge-response can be an excessive overhead on remote procedure calls and store-and-forward systems. For these reasons, general purpose distributed systems should provide both timestamp and challenge-response facilities, and the latter can support the former via synchronisation protocols.

021220 'Freshness Assurance of Authentication Protocols'
KY Lam, D Gollmann, *Proc. ESORICS 92 - Springer LNCS v 648, pp 261 - 271*
The rôle of time in assuring freshness in distributed authentication protocols is discussed. Timestamps are better than sequence numbers or random challenges from the systems point of view, but worse from the point of view of security. However, time has additional uses such as limiting the validity of credentials. Kerberos and Selane are discussed as examples.

021221 'A Framework for Composition of Security Models'
J Landauer, T Redmond, *Proc Franconia 92 pp 157 - 166*
The authors consider the design of a modular operating system and suggest that different components may have been subject to different forms of analysis during their design. They consider certain components of the TMach (Trusted Mach) operating system and consider a composition theorem to analyse their combination.

021222 'A Look at Multipolicy Research Today and Some Proposed Directions for Tomorrow'
EV Leighninger, *ACM SIGSAC Review v 10 pp 12 - 17*
Information systems are often built to support multiple and conflicting human activities, and therefore end up being governed by multiple security policies. An overview is given of research topics in this field, together with suggestions for future work.

021223 'A Record Oriented Cryptosystem for Database Sharing'
CH Lin, CC Chang, RCT Lee, *Computer Journal v 35 no 6 pp 658 - 660*
A variant is proposed of the Davida-Wells-Kam system, in which database records are encrypted by linear transformations and combined using the Chinese Remainder Theorem.

021224 'Attribute based data model and polyinstantiation'
TY Lin, *IFIP 92 pp 472 - 478*
Where cover stories are used to solve the polyinstantiation problem, then the ratio of real data to cover stories can become low. A new model of cover stories is presented, based on attribute-based data modelling. The effect is that real data and cover stories should be stored separately at each level.

021225 'An inter-bridge security protocol'
R Lipp, R Posch, *Computer Networks and ISDN Systems v 25 (92) pp 496 - 500*
The authors discuss university security requirements, and the problem posed by the mix of highly insecure student networks and administrative systems with confidential information. They propose internetwork security using bridges, with the bridge idle time being used to generate keystreams using RSA.

021226 'Private Lock Management'
D Loment, *DEC Cambridge Research Lab report CRL 92/9*
This paper investigates ways of cutting the coordination cost of locking records in distributed database systems. Protocols are proposed to coordinate local lock managers. These raise a number of questions about hierarchy and granularity, which can be used in various ways to improve the trade-off between concurrency and lock overhead.

021227 'Fine Grained Object Protection in Unix'
MR Low, B Christianson, *ACM Operating Systems Review v 27 no 1 (92) pp 33 - 50*
This article describes how fine grained protection can be provided under Unix for object ori-

ented systems. The problem is to control the invocations of the methods of one object by the methods of another and to prevent cross-domain problems; the solution is to keep all the methods in one domain and invoke them using stub routines, which can be allocated Unix permissions in the usual way. Meanwhile all the instances of a given object are kept in a separate domain.

021228 'An Example Complex Application for High Assurance Systems'
FL Mayer, SJ Padilla, *Proc 15th NCSC pp 153 - 164*

Multi-level applications can and should be built without trusted code: an architecture is proposed for a multi-level secure windowing system based on replication of window servers which receive input from a trusted device manager (assumed to be part of the operating system). Visible labels are not provided on windows because the windows are already labeled in memory by the TCB, although this labeling is not visible to a user. Cut and paste upwards is allowed. This unproven system architecture has the potential for higher assurance than TRW's prototype windowing system, but at a significant functionality cost.

021229 'The Channel Capacity of a Certain Noisy Timing Channel'
IS Moskovitz, AR Miller, *IEEE Trans. on Information Theory v IT-38 no 4 (1992) pp 1339 - 43*

A covert timing channel may suffer noise generated by time sharing delays as other users compete for resources. Two strategies for communicating in the presence of this noise are analysed and the resulting channel capacity is determined.

021230 'A unified model for security and integrity in relational databases'
A Motro, *Journal of Computer Security v 1 no 2 (1992) pp 188 - 213*

This paper discusses the security mechanisms of existing relational databases, including System R and Ingres, and presents a new model which unifies security and integrity properties by phrasing the latter as views to which permissions are never granted. The proposed scheme can use knowledge about the access rules to deduce what subtransactions of a forbidden request may be allowed; but one must be careful that this does not leak information. It is shown how this 'view inference problem' can be treated formally.

021231 'Operational Support of Downgrading in a Multi-Level Secure System'
D Nelson, G Factor, J Studt, M Yelton, S Heffern, F Kramer, *Proc 15th NCSC pp 467-472*

An operational multilevel system is described which needs to perform routine downgrading of data in a relational database. The application uses polyinstantiation for cover stories, so simply relabelling tuples could cause integrity problems. An database-independent application is sketched which allows authorized users to downgrade information without being intimately aware of the database design. Special attention is paid to auditing so a historical view of the downgraded information is available.

021232 'Generation of secure passwords by the user'
E Piller, *IFIP 92 pp 518 - 524*

The author suggests various password generation algorithms which can be used to construct long, seemingly random passwords from remembered words, tunes, dates and so on. The procedure can be further complicated by displaying a 26 by 26 Latin square on the logon screen which can be used to guide the user through a manual challenge-response routine.

021233 'An Open Commit Protocol Based on a Model for Consistency Checking'
K Rothermel, *Stuttgart University Fakultät Informatik Fakultätsbericht 12/92*

Most proposed commit protocols assume honest players. However, in open distributed systems on can assume that untrusted nodes exist. A protocol is proposed which tolerates arbitrary failures in the untrusted domain, and transient failures in the trusted domain, while guaranteeing that all trusted participants terminate in a way that preserves the trusted domain's consistency. This is achieved by means of consistency checking, and the protocol uses only two more messages per commit than the traditional two-phase commit protocol.

021234 'Eliminating Polyinstantiation Securely'
RS Sandhu, S Jajodia, *Computers and Security v 11 no 6 (Oct 1992) pp 547 - 562*
This article describes the polyinstantiation problem, and suggests a solution in the form of 'restricted polyinstantiation', in which low level users see objects in use by high level users with the attribute 'restricted'. It is argued that this is a pragmatic approach, and its syntax is discussed.

021235 'Polyinstantiation for Cover Stories'
RS Sandhu, S Jajodia, *Proc. ESORICS 92, pp 307 - 328*
This paper discusses the options for managing conflicts between security and integrity in multilevel databases, and show in particular that entity polyinstantiation can be eliminated by a discipline of cover stories. If, for example, a ship has a classified spying mission, one would generate a corresponding unclassified exploration mission as a cover. The semantics of the approach are discussed; polyinstantiation can be controlled in an intuitive way by entities to whom it is visible.

021236 'A Multilevel Secure Database Management System Benchmark'
LM Schlipper, J Filsinger, VM Doshi, *Proc 15th NCSC p 399 - 408*
Existing benchmarks are inadequate for judging secure database performance because they fail to take the effects of security related factors into account: different architectures are affected differently by security label distributions, by the cost of performing access checks, and by measures to combat covert channels, polyinstantiation, and so on. A common benchmark methodology is described: it involves adding security labels to synthetically generated data and running queries. However, different vendors have extended the relational model in different ways, and this makes it hard to write a portable benchmark.

021237 'Towards a Policy-Free Protocol Supporting a Secure X Window System'
M Smith, *Proc 15th NCSC pp 717 - 727*
Multi-level secure versions of the X Window System can be constructed without embedding the security policy in the X server. Rather, the X server can be extended by invoking a Policy Defining Client (PDC) at each place where a security policy decision is to be made. This way, the X server need be trusted only to query the PDC when needed and follow its instructions, not to make security policy decisions. Extensions to the X protocol to support interactions between the X server and PDC, and between the X server and other clients are described.

021238 'Multilevel Security Issues in Distributed Database Management Systems III'
B Thuraisingham, HH Rubinovitz, *Computers and Security v 11 no 7 (11/92) p 661 - 674*
This article discusses possible architectures for multilevel security in database management systems, and extends previous work to heterogeneous environments. In this case, one cannot assume data replication, and so it is not always possible for transaction requests to be serviced at a node with the same security classification as the user. This can introduce covert channels, and a number of other potential pitfalls in query and transaction processing are also discussed.

021239 'Secure interoperability of trusted database management systems'
B Thuraisingham, *ACM SIGSAC Review v 10 pp 8 - 11*
This paper presents an overview of the problems involved in getting trusted databases to work together. They include: different data models, interpretations and integrity constraints; different algorithms for transaction processing (including different query languages); different semantics at different levels of classification; and different classifications of the same entity.

021240 'Realisation of the Bell-La Padula Security Policy in an OSI-Distributed System Using Asymmetric and Symmetric Cryptographic Algorithms'
J Verschuren, R Govaerts, J Vandewalle, *Proc Franconia 92 pp 168 - 178*
The authors consider cryptographic techniques for enforcing a security policy such as that proposed by Bell and La Padula in a system where the components are connected by an insecure

network. They suggest that both symmetric and asymmetric cryptosystems should be used and discuss key distribution. They propose minimising the number of keys as a design goal.

021241 'Relational Database Security'

LL Vetter, *Computer Fraud and Security Bulletin Nov 92 p 7 - 12*

This is, firstly, an elementary introduction to database security issues including mandatory access controls, rôles and views, multilevel security, polyinstantiation, and the interface with operating system security; and secondly, a description of the ORACLE security strategy and user consultation procedures.

3 Security Management and Policy

021301 'VISA confronts the con men'
N Achs, *Cards International, 20 Oct 1992, pp 8 - 9*
Up till 1989, almost all credit card counterfeiting was of the card embossing, but since then magnetic strip counterfeiting has grown to half the total, or almost $100m in 1992. By April 1993, all new VISA cards will incorporate a control verification value, or CVV, which is a crypto checksum on the strip. VISA sees the long term solution to fraud as being fully online authorisation and will introduce transaction analysis screening during 1993. This will spot suspect transaction patterns and will take place in the interbank part of the network. The number of countries needing to use smartcards is expected to dwindle as communications improve.

021302 'Reference Model for Data Management Security and Privacy'
S Albert, VA Ashby, SE Hicks, *ACM SIGSAC Review v 10 pp 44 - 62*
This article presents a model whose goal is to refine the security concepts used in data management systems. It describes the necessary differences from the standard security models, and the problems which have to be solved to provide confidentiality, availability and integrity.

021303 'Assessing Modularity in Trusted Computing Bases'
JL Arnold, RJ Bottomly, DB Baker, DD Downs, F Belvin, S Chokhani, *Proc 15th NCSC pp 44 - 56*
TCSEC B2 (and above) systems must meet modularity requirements. Six modularity attributes have been defined by a working group: code cohesion (how closely related code is within a module or function), code complexity, code and data coupling, data cohesion (how closely related are the data within a structure), duplicate code and data, and extraneous code and data. For each attribute, criteria are specified for judging modularity, and a minimum level is established to meet the B2 evaluation class.

021304 'Case Study - James Capel's recovery from the city bombing'
D Austin, *Computer Audit Update, June 1992*
On April 10 1992, an IRA bomb went off in London only 200 feet from the building housing the dealing and computer rooms of stockbroker James Capel. The latter was spilt in two and the former had a wall destroyed. The article describes how a backup site was activated, and the main facility restored within three days.

021305 'Security Issues in EDI Environment'
S Banerjee and DY Golhar, *IFIP 92 pp 457 - 463*
EDI systems are vulnerable to disclosure, modification, masquerade, repudiation and service denial. A variety of encryption and network management techniques can be used to control the risks. Furthermore, a comprehensive contract is needed in order to give legal force to EDI documents, and this may be bilateral or multilateral.

021306 'Security policy'
SH Banks, *IFIP 92 pp 464 - 471*
This article presents a model security policy for use by commercial and other organisations. It covers management controls, change control, copyright enforcement, input document control, physical security, access controls, backup and contingency planning.

021307 'Risk and vulnerability in an information and artificial society'
J Berleur, *IFIP 92 pp 294 - 313*
This paper discusses the nature of technological risk, starting off with its treatment in myth and literature, and continuing with the effects of program trading in Wall Street in the crash of 1987 and cases of system malfunctions in hospitals. It discusses the highly complex nature of social

risk, and argues that security measures include not just technical and organisational issues, but also legal, social and economic ones.

021308 'Data Security for Personal Computers'
P Bicknell, *Proc 15th NCSC pp 101 - 110*

This paper surveys the threats against IBM PCs and the existing solutions. Solutions can be divided into physical and data protection. Physical security can be achieved using locks or by removable media, while data protection is subdivided into domain isolation and anti-viral capabilities. Domain isolation introduces features similar to those found in minicomputer and mainframe operating systems, while anti-viral capabilities may be pro-active (using scanners to detect viruses) or reactive (using checksums to detect corruption or suspicious patterns of behavior arising once an infection has occurred).

021309 'Psychology of Computer crime'
K. Buckner, J Fielding, *Computer Audit Update, Sep 1992 p 12 - 15 (part 1) and Oct 1992 (part 2) p 12 - 17*

These articles discuss the different approaches to classifying computer crime, such as by offence (theft, fraud, sabotage) or motive (recreation, craft, project, profession), and examines corporate thinking about this. Threats are diverse and evolving, and different studies have yielded quite different profiles of 'typical computer criminals'. The authors conclude that no usable distinction has yet been found between criminals and noncriminals.

021310 'A Local Area Network Security Architecture'
LJ Carnahan, *Proc 15th NCSC pp 340 - 349*

This article describes how to evaluate and improve LAN security. A five step process is proposed which defines the LAN configuration, determines the threats to it, selects security services, develops priorities, and implements the security services. This 'cookbook' approach is useful for both existing LANs as well as systems still being designed, and security services (such as identification, authentication, access control, and data integrity) are explained.

021311 'Computer Contingency Plans and the Auditors: A Survey of Businesses Affected by Hurricane Hugo'
MJ Cerullo, RS McDuffie, *Computers and Security v 11 no 7 (11/92) p 620 - 627*

This article presents a study of 41 companies in the Charlestown area, which was devastated by hurricane Hugo in 1989. 56% of the 18 companies which had a contingency plan were unable to process critical accountancy jobs, compared with 61% of the 23 which had no such plan.

021312 'ITSEC - an ongoing process'
Computer Audit Update, Oct 1992, pp 3 - 8

This article summarises a seminar on ITSEM which was organised by the EC commission in Brussels on 8-9 September 1992. Feedback on ITSEC/ITSEM included the criticisms that ITSEM should be more concise; it should be more consistent with ITSEC; it should be more usable; it should be part of wider quality criteria; that more work is needed on functionality classes; and that it is about generating documents, not methodology (but the latter would conflict with market principles anyway). A revised ITSEM is due by the first quarter of 1993.

021313 'Human Factors in Computer Security'
I Dabipi, H Yaghi, I Qasem, *Proc IFIP 92 pp 322 - 328*

Network security and access control are only two parts of computer security: the vital, and often neglected, third component is organisational security. Ninety eight percent of threats are internal to the organisation, and these can be motivated by the technical challenge, game playing, or curiosity. As about one third of internal violations are accidental, these also have to be provided for. An element of randomisation, both of access privileges and of job rotation, can be useful.

021314 'LAN Security Standards'

J David, *Computers and Security v 11 no 7 (11/92) p 607 - 619*

This article provides a management level overview of LAN security problems and sources of security products and advice. It also gives a glossary of terms and conventions used in discussing this topic.

021315 'How to get the better of the computer fraudster'

J Essinger, *Financial Technology Insight, Sep 92, pp 9 - 14*

Checklists are given for the various phases of a computer fraud investigation, including selecting investigators, securing evidence, limiting losses, remedial action, following audit and money trials, and identifying and interviewing suspects.

021316 'Kid Crypto: Cryptography for the Young'

MR Fellowes, N Koblitz, *Proc Crypto 92*

This article discusses ways of introducing crypto concepts to the young and non-technical, using crayons rather than computers. These techniques can be used to introduce concepts of algorithms, randomisation, graphs and codes.

021317 'Addressing Vulnerability and Privacy Problems generated by the Use of IT Security Mechanisms'

S Fischer-Hübner, L Yngström and J Holvast, *Proc IFIP 92 pp 314 - 321*

IT security mechanisms often introduce administrative controls which conflict with users' privacy. Access control mechanisms reveal personal information about the users' status; these, together with intrusion detection systems, may be abused to monitor employee performance. The data protection laws of a number of countries prevent data collected for one purpose from being used for a different one. Anonymity is one way to prevent this: one can allow system users to choose aliases.

021318 'Spymasters fear bug-proof telephones'

B Fox, *New Scientist no 1858 (Jan 1993) p 19*

This article reports that exports by European equipment vendors of GSM cellular phones to the Middle East are being blocked, because GCHQ in Britain and the FBI in the USA fear that the encryption algorithm used, called A5 and described as similar to DES, will take 'huge amounts of computer power' to crack and thus hinder law enforcement. As a result, the UK Department of Trade and Industry has asked for a different export standard, with weaker encryption or none at all. This could result in the mobile phone market being captured by US or Japanese vendors.

021319 'Evolving Criteria for Evaluation: The Challenge for the International Integrator of the 90's'

V Gibson, J Fowler, *Proc 15th NCSC pp 144 - 152*

The existence of three sets of evaluation criteria (U.S. TCSEC, Canadian CTCPEC, and European ITSEC) leads to complexity for product vendors, and systems integrators attempting to mix and match products to build systems are further stymied by the lack of reciprocal acceptance of evaluations. Export control slows the integrator, as does the continual revision of criteria. The burden could be reduced by reciprocal evaluations and a single international evaluated products list.

021320 'Breach of System Security and Theft of Data: Legal Aspects and Preventive Measures'

F Gilbert, *Computers and Security v 11 no 6 (Oct 1992) pp 508 - 517*

This article surveys the current state of US federal and state law on computer crime and describes some recent cases (Riggs, Neidorf and Revlon). It also discusses legislation proposed by the Justice Department in response to computer viruses.

021321 'ASAX: Software Architecture and Rule-Based Language for Universal Audit Trial Analysis'
N Habra, B le Charlier, A Mounji, I Matthieu, *Proc. ESORICS 92, pp 435 - 350*

This article describes ASAX, an audit trial analysis tool which is implemented under the Siemens operating systems SINIX and BS-2000, and allows one-pass analysis of audit trails generated by them. It uses a language, RUSSEL, in which rules are declared which describe patterns of events, such as sequences of failed logins, which must be examined further or brought to the operator's attention.

021322 'Provably Weak Cryptographic Systems'
J Higgins, C Mashayeki, *Proc 15th NCSC pp 523 - 530*

The authors of this paper propose that US personal computer software vendors should adopt a version of DES which would be weakened enough to have export controls waived but strong enough to satisfy users.

021323 'Perspectives in Information Technology Security'
HJ Highland, *Proc IFIP 92 pp 440 - 446*

Information security efforts have in the past focussed on hardware and software, with disappointing results. The military model, which has gained acceptance in business as well, is not cost-effective, as the human factor has been neglected. A number of abuses are chronicled; it turns out that the average tenure of computer security managers at US government agencies is only seven months. This prevents serious investment in education and training, which is the real need: many security breaches are caused by careless implementation or negligent operation.

021324 'Reducing society's vulnerability as computers and networks proliferate'
LJ Hoffman, *Proc IFIP 92 pp 554 - 563*

This article reviews vulnerability of computer systems and points out a steady weakening of management control, as mainframes and minis are replaced by PCs and networks under no specific control. By 2010, computer networks will probably have subsumed both telephone and television, so the security management and standards problems will need closer attention.

021325 'Computer fraud - the expanding business'
C Hood, *The Computer Bulletin v 4 pt 4 pp 27 - 29*

This article describes the common types of computer fraud, and reviews the use of access control, audit and management policies to counter them.

021326 'Getting back up'
M Horten, *Banking Technology, June 1992, pp 47 - 49*

This article surveys the effects of two city centre disasters - a bomb blast in London in April and a flood in Chicago in May. These affected a number of companies' computers, but did not lead to any system disasters; electronic records turned out to be much more resilient than paper ones. The key factor in system recovery was the rapid response of equipment vendors, telecom companies and backup facility suppliers.

021327 'Metapolicies I'
HH Hosmer, *ACM SIGSAC Review v 10 pp 18 - 43*

Security policy conflicts are the norm rather than the exception in complex systems, and must be resolved using metapolicies, or 'policies about policies'. Most metapolicies in existence are invisible and implicit; the problem of how to make them explicit is discussed.

021328 'Metapolicies II'
HH Hosmer, *Proc 15th NCSC pp 369 - 378*

Metapolicies, or 'policies about policies', are a way of expressing complex interrelationships between security policies. Existing metapolicies are often implicit, and making them explicit is hard. However, doing this forces recognition of many different aspects that make up a policy. An example shows nine metapolicies which make up a particular interpretation of the Bell-LaPadula simple security policy. Because metapolicies can be used to show relationships, they are useful in coordinating policies in both government and commercial organizations.

021329 'The Multipolicy Paradigm'

HH Hosmer, *Proc 15th NCSC pp 409 - 422*

A new paradigm is needed for integrating multiple, and potentially contradictory, security policies. While TDI, TNI, and ITSEC allow for multiple policies, all require that they be integrated into a single coherent whole. This is unreasonable: it is inflexible and unrealistic, requires manual review when exchanging data with systems enforcing other policies, and gives poor performance. Multipolicy systems are proposed as the solution, with various means of resolving the conflicts between policies. Evaluation of products and policies should be separated, with certifiers giving approval to use particular combinations of policies and products.

021330 'Banks still court disaster'

International Banking Systems, Feb 92, pp 9 - 11

This article looks at disaster recovery in the UK banking sector. Recovery services are provided by equipment vendors and specialists, but of the 600 banking users of IBM midrange systems in London, only about half are covered by one of these facilities.

021331 'Security measures, standardisation and the law'

H Kaspersen, *Proc IFIP 92 pp 393 - 399*

A number of countries make the implementation of information security measures into a legal obligation on operators of certain computer systems, whether under national security, computer crime or data protection legislation. An alternative approach is to set standards and facilitate the emergence of a market in security products and systems, such as with the EC ITSEC programme. However legal standards should be set separately as they operate on a different level of abstraction.

021332 'Legal Aspects of Data Security'

W Kilian, *IFIP 92 pp 377 - 384*

Lawyers must be involved in establishing security categories, designing security standards and introducing internationally binding conventions and rules, or all sorts of dispute may arise in the future about the evidentiary value of electronic objects and of the output of systems. National laws and international conventions are still deficient in many respects.

021333 'The IT Security Evaluation Manual (ITSEM)'

Y Klein, E Roche, F Taal, M Van Dulm, U Van Essen, P Wolf, J Yates, *Proc 15th NCSC pp 300 - 309*

ITSEM sets out the methodology for performing an ITSEC evaluation. A major goal of ITSEM is to enable mutual recognition of evaluation results, so these results need to be predictable and reliable, regardless of the evaluation team. Examples are provided showing the ITSEM approach to penetration resistance (based on objective measures of time, inside collusion, equipment, and expertise required) and vulnerability assessment (based on a checklist of potential weaknesses). Evolution of the ITSEM is continuing.

021334 'Phreaking recognised by Directorate General of France Telecom'

HM Kriz, *Chaos Digest 1.03 (Jan 93)*

Over a thousand subscribers who use illegally imported cordless telephones in the northern suburbs of Paris have received elevated phone bills as a result of the poor authentication provided by these devices. 'Pirates' with such devices make long distance calls from nearby the subscribers' houses. An information campaign on the threat is being planned.

021335 'Network(er)s at risk - The Fairy-Tale Invulnerability of Computer Supported Work'

H Kubicek, *Proc IFIP 92 pp 400 - 418*

This article describes the German government IT security handbook, which sets out a procedure for federal government agencies to develop their own information security concept. This is much more thorough than ITSEC, and covers the organisational as well as technical issues. The article also highlights security versus privacy dilemmas, and suggests that such standards should also explicitly require the policy setter to take into account the interests of various groups in the system's functionality.

021336 'A Note on Compartmented Mode: To B2 or Not B2?'

TMP Lee, *Proc 15th NCSC pp 448 - 458*

Compartmented mode can be used when users of a computer system are cleared to the highest level of information on the system, but do not have formal access to all compartments. The author explains the rationale for this, but argues that the risks involved are too great to rely on the minimal protection afforded by C2 and B1 systems, which have no requirement for resistance to a determined attack.

021337 'Security in Local Area Networks'

P Lipp, *Proc IFIP 92 pp 486 - 493*

This article presents an overview of LAN security, and how eavesdropping, masquerade, modification and service denial attacks can be carried out on ethernet and token-ring type networks. The countermeasures are improving awareness, standardising security protocols, building security functions into applications, and building firewalls between different networks. The Graz university network is described as an example.

021338 'Minitel Pirates Work at France Telecom'

W Losh, *Chaos Digest, v 1.03, Jan 93*

Eight employees have been accused of abusing the Minitel system in France with damages sustained by ministries (including the foreign ministry) amounting to millions of francs. The compromise was discovered on investigating a suspiciously high Minitel bill.

021339 'Local area networks - security and access control'

W Murray, *Computer Fraud and Security Bulletin Dec 92 p 10 - 16*

This article presents an overview of the security issues involved in managing LANs and network operating systems. It describes typical access control features and common weaknesses such as eavesdropping, lack of local logons, and lack of compartmentation in server software. The last two features in particular make LANs vulnerable to trojan horse attacks. A checklist of actions for security managers is included.

021340 'Automation-Related Complacency: A Source of Vulnerability in Contemporary Organisations'

S Parasuraman, IL Singh, R Molloy and R Parasuraman, *Proc IFIP 92 pp 426 - 432*

Operator complacency arises when systems are highly reliable, and especially when their inner workings are not accessible or understood. A survey was carried out of attitudes toward automation, including CAT scanners, automatic teller machines and videocassette recorders, which indicated that the complacency potential was also a function of individuals, and depended on sex, age and education. Its pattern was similar to that of computer anxiety and the pattern of microcomputer use.

021341 'Systemic Methods for the Analysis of Failure'

G Peters, J Fortune, *Systems Practice v 5 (Oct 92) pp 529 - 542*

Most major disasters have involved a system failure of some kind. Thus a system approach to reliability design is highly desirable. One such is presented, and involves analysing not just the system's process behaviour, but also its interaction with the environment and the social factors affecting its users.

021342 'Issues to Consider When Using Evaluated Products to Implement Secure Mission Systems'
WR Price, *Proc 15th NCSC pp 292 - 299*
Despite the increasing availability of TCSEC evaluated products, few operational systems use them (and even fewer use them properly). Such products are no substitute for thorough system engineering: the design of operational systems should include a security requirements specification which is properly conducted rather than being a paraphrase of any seemingly relevant Orange Book requirements. Only then can one tell whether evaluated products are appropriate. It turns out that there is frequently a mismatch between capabilities provided and those needed, including limiting aggregation, time-based downgrading, and support for trusted applications.

021343 'Randomised Algorithms in "Primitive" Cultures'
J Shallit, *SIGACT News v 23 no 4 (1992) pp 77 - 80*
Randomised algorithms have recently found many applications in cryptology and elsewhere in computer science. However they are not new; primitive cultures also use them, and examples from tribes in Canada and Central Africa are discussed. In particular, the use of a random oracle to direct hunting seems to work by preventing any anticipatory response by the prey.

021344 'On Blind Signatures and Perfect Crimes'
B von Solms, D Naccache, *Computers and Security v 11 no 6 (Oct 1992) pp 581 - 583*
If blind signatures as advocated by Chaum had been implemented, they would have prevented the apprehension of a kidnapper in Japan who had opened an ATM account in a false name in order to collect the ransom. This shows that fear of 'Big Brother' should not be the only social consideration in assessing such systems.

021345 'The Virus Authors Strike Back'
A Solomon, *Computers and Security v 11 no 7 (11/92) p 602 - 606*
Anti-viral products can be classified as scanners, integrity checkers and behaviour blockers. The latter two, especially, need to discriminate between viruses and other phenomena in order to be useful. There are a number of traps for unwary users of anti-viral products, including polymorphic and stealth viruses.

021346 'Vulnerability of computer systems: establishing organisational accountability'
I Wagner, *Proc IFIP 92 pp 433 - 439*
The practical problems of implementing technical security measures are highly organisational in nature, and many problems arise because people fail to integrate inputs from diverse sources. Machine-generated warnings are often considered separately from other kinds of information.

021347 'Legal Control of IT Misuse: The Limited Relevance of the Criminal Law'
M Wasik, *IFIP 92 pp 385 - 392*
This paper reviews the UK Computer Misuse Act of 1990, which makes it an offence to gain unauthorised access to programs or data stored in a computer, and to deliberately corrupt such programs or data whether by using viruses or otherwise.

021348 'MHS security - a concise survey'
SC Wu, *Computer Networks and ISDN Systems v 25 (92) pp 490 - 495*
This article reviews the threats to message handling systems, relevant security standards, and the various publicly funded research projects underway in this field in Europe and the USA.

4 Formal Models and Methods

021401 'The Expressive Power of Multi-Parent Creation in Monotonic Access Control Models'
P Ammann, R Lipton, RS Sandhu, *Proc Franconia 92 pp 148 - 156*

The authors contrast two security models - the Schematic Protection Model (SPM) and the Extended Schematic Protection Model (ESPM). By highlighting their differences they show how expressions in one model may be difficult to express in the other; in particular they assert that SPM is less expressive than ESPM.

021402 'UEPS - A Second Generation Electronic Wallet'
RJ Anderson, *Proc. ESORICS 92, pp 411 - 418*

This paper describes the design and verification of a smartcard based eftpos system. The verification was carried out using the BAN logic, which had to be extended to cope with key chaining. Various other extensions of BAN which deal with freshness and chaining are discussed. The verification exercise showed that such logics can be used at the application level as well as the system level; and they can be very useful if they are compact enough to be manageable. BAN is manageable in this sense, but the GNY logic is not. Furthermore, an error is exhibited in the GNY treatment of freshness.

021403 'Formal Models of IT Security'
F Barry,*The Computer Bulletin v 4 pt 4 (Sep 92) pp 25 - 26*

This article gives an entry-level description of the formal methods used in verifying operating system kernel designs, and gives an explanation of dominance and the Bell-La Padula model.

021404 'Cryptographic protocols provable secure against dynamic adversaries'
D Beaver, S Haber, *Proc Eurocrypt 92*

The authors review the definition of resilience and some of its applications for proving security of cryptographic protocols as was done in the first author's Crypto '89 paper. They then use this technique for multiparty cryptography and prove that their protocol is secure against a dynamically chosen minority. The model allows participants to erase portions of memory.

021405 'A Formal Framework for Authentication'
C Boyd, *Proc. ESORICS 92, pp 273 - 292*

This paper investigates the formalisation of cryptographic protocols using the OSI tool LOTOS. It presents type descriptions for protocol primitives such as secrets and nonces, and shows how to specify the Needham-Schroder protocol as an example. The crux is accepting an authentication as strong if it contains a signature and freshness.

021406 'An Analysis of Some Delegation Protocols for Distributed Systems'
C Calvelli, V Varadharajan, *Proc Franconia 92 pp 92 - 110*

Varadharajan, Allen, and Black described some delegation protocols. The present paper uses techniques proposed by Abadi, Burrows, Lampson, and Plotkin, and the logic developed by Kailar and Gligor, to analyse these protocols in more detail.

021407 'Partial Belief and Probabilistic Reasoning in the Analysis of Secure Protocols'
EA Campbell, R Safavi-Naini, PA Pleasants, *Proc Franconia 92 pp 84 - 91*

The authors propose an extension to the BAN (Burrows, Abadi, and Needham) logic; their extension allows users to assign probabilities to certain beliefs. This leads to certain problems that they discuss in their conclusion.

021408 'A Formal Definition of Computer Worms and Some Related Results'
FB Cohen, *Computers and Security v 11 no 7 (11/92) p 641 - 652*

The author's formal definition of a computer virus is reviewed, and extended to computer worms. A number of theorems are presented, and the characteristics of worms in multiprocessor systems are discussed.

021409 'A Logic for Reasoning About Security'
J Glasgow, G MacEwen, P Panagaden, *ACM Transactions on Computer Systems v 10 no 3 (Aug 92) pp 226 - 264*

This paper sets out to formalise reasoning about knowledge, permission and obligation. Security logic is seen as the interaction of possible worlds with time, and becomes quite complex: security in general is liveness plus safety, where privacy is basically a safety feature and integrity is more a liveness property. In addition, integrity is an obligation to know (for example, a ledger must know its previous entries); privacy means that each subject is permitted to know everything he does know. Building a comprehensive theory entails introducing both temporal and deontic operators; the former include 'always', 'eventually' and 'sometimes', while the latter are based on 'obligatory' and 'permitted'. Its application to the Clark-Wilson model is described.

021410 'Some Laws of Non-interference'
J Graham-Cumming, *Proc Franconia 92 pp 22 - 33*

The author proposes nine laws, expressed in CSP, that characterise non-interference. He wishes to examine whether systems that do not exhibit interference can be composed into a network of systems that does. This work is still in progress.

021411 'The use of formal methods in data security standards'
A Harry, *NPL report DITC 205/92*

Formal specification of the algorithms used in data security standards is highly recommended, owing to the many and subtle possibilities for ambiguity and misconstruction, of which examples are given.

021412 'VDM specification of the MD4 message digest algorithm'
A Harry, *NPL report DITC 204/92*

This contains a formal specification of the MD4 algorithm in VDM, as an example of how such a specification can lead to an unambiguous standard which is easy to implement in a variety of programming languages. Possible ambiguities in the original specification are highlighted, including padding and constants, which were resolved by examining the original 'c' implementation.

021413 'A RAISE specification of the MD4 message digest algorithm'
A Harry, *NPL report DITC 206/92*

This report contains a specification of MD4 in RAISE, and is otherwise similar to the VDM specification mentioned above.

021414 'VDM specification of the secure hash algorithm'
A Harry, *NPL report DITC 212/92*

This contains a formal specification of the secure hash algorithm in VDM, and is similar to the work on MD4 mentioned above. In this case the only ambiguity found was in one of the variable assignments.

021415 'Verification and Modelling of Authentication Protocols'
RC Hauser, ES Lee, *Proc. ESORICS 92, pp 141 - 154*

An extension of the BAN logic is presented which differentiates between objects which have been freshly created, and objects which have been freshly used. Freshness can be transferred from the first of these to the second, and if an encrypted message contains a freshly created item, then the key can be considered freshly used. An implementation of this logic is also reported.

021416 'Formal Methods and Automated Tool for Timing-channel Identification in TCB Source Code'

JD He, VD Gligor, *Proc. ESORICS 92, pp 57 - 75*

A covert channel can be brought into existence where there exists a synchronisation mechanism (such as resource exhaustion) together with cooperating high and low level processes. The source code of these processes can be checked automatically for possible cooperation: wherever a high level process can change the system state in a way which a low level process can view, we must check whether the possible information flow is illegal in an associated model. Although this methodology may detect all storage channels, hardware dependencies mean that it cannot be as effective for timing channels.

021417 'Foundations of Intrusion Detection'

P Helman, G Leipins, W Richards, *Proc Franconia 92 pp 114 - 120*

The authors divide computer use into two categories: normal and misuse. They suggest that intrusion detection involves discovering those processes that fall into the latter category. Some detection systems use statistical techniques to discover suspicious behaviour; these may miss isolated incidents. The authors claim that the problem of discovering such incidents is NP-hard.

021418 'Formal Specification of Security Requirements using the Theory of Normative Positions'

AJI Jones, M Sergot, *Proc. ESORICS 92, pp 103 - 121*

The theory of normative positions evolved as a discipline in jurisprudence. It seeks to clarify concepts such as duty, privilege, immunity and power by using operators in modal logic such as 'A is obliged to do x' and 'A brings it about that x'. It can be used to clarify security requirements, and extends previous formalisms in various ways: for example, it enables a designer to differentiate between active and passive obligations. An overview of the theory is given, together with a sketch of how it may be applied to Ting's problem of the security specifications needed for a hospital records system.

021419 'Authentication in Distributed Systems: Theory and Practice'

B Lampson, M Abadi, M Burrows, E Wobber, *ACM Transactions on Computer Systems v 10 no 4 (Nov 92) pp 265 - 310*

The authors propose and develop an access and authentication logic for access requests in distributed systems. These may have a complex source: a user might typically run an application on a workstation, and this application in turn may request access to an object held on a remote server. Formal analysis of such requests must cope with delegation, variation in communication paths and program loading, as well as the usual authentication issues. The proposed logic treats as principals both named entities and communication paths; its primitives are statements of the form 'A says (B says X)'. An access request is only granted if a proof of an access right can be constructed; this provides a formal basis for auditing. This logic was used to design DEC's DSSA.

021420 'A Classical Automata Approach to Noninterference Type Problems'

IS Moskowitz, OL Costich, *Proc Franconia 92 pp pp 2 - 8*

The authors are concerned with covert channels in a computer system that supports concurrent processes of differing security levels or clearances. They assert that a 'Secure Nondeterministic Automaton' is useful for identifying unauthorised probabilistic channels.

021421 'Causal Security'

M Mowbray, *Proc Franconia 92 pp 54 - 62*

A number of systems fail to meet existing formal definitions of security because of timing effects, eg when an audit trail is written before a transaction is processed, or where time in a distributed system is not well defined. The author proposes basing security models on causation instead of time.

021422 'Unwinding and the LOCK Proof Referees Study'
SR Murphy, S Crocker, T Redmond, *Proc Franconia 92 pp 9 - 21*

SCTC (previously Honeywell) defined a formal method for a secure system that they called LOCK, which was defined using the Gypsy Development Environment and distributed for independent review. This paper was the result of one of these reviews; it clarifies then examines the 'unwinding theorem'.

021423 'Modelling and Analyzing Cryptographic Protocols Using Petri Nets'
BB Nieh, S Tavares, *Proc. Auscrypt 92,*

Petri nets have been widely used to analyse and model communications protocols; they can be adapted simply to crypto protocol problems. An overview of the basic theory is given, and this is developed to show flaws in protocols by Burns and Mitchell, Meyer and Matyas and Mitchell and Walker.

021424 'On Requirements and Security in a CCIS'
C O'Halloran, *Proc Franconia 92 pp 121 - 134*

The author uses a hypothetical Command and Control Information System as an example to demonstrate his calculus of information flow, proposed in a previous paper.

021425 'An Algebraic Approach to Non-interference'
S Pinsky, *Proc Franconia 92 pp 34 - 47*

Haigh and Young proposed a 'view identical' problem concerned with information leakage in a multi-level secure system. The author proposes conditions based upon a state transition matrix that he claims are necessary and sufficient for solving this problem.

021426 'A Nonmonotonic Typed Multilevel Logic for Multilevel Secure Data/Knowledge Base Management Systems - II'
B Thuraisingham, *Proc Franconia 92 pp 135 - 146*

In a previous paper the author described a logic called Nonmonotonic Typed Multilevel Logic (NTML). A subset of NTML has been specified called NTML-Prolog. The author gives several examples of how the logic and the NTML-Prolog programming language might be applied to multi-level databases.

021427 'The authenticability of public key protocols'
C Tian, *Chinese Journal of Computers v 15 no 2 (92) pp 144 - 152*

This paper considers the problem of preventing masquerade in public key protocols. As an example, a protocol which can allow masquerade is analysed, and a formal definition of authenticability is proposed. This is used to prove the security of a practical protocol.

021428 'Separating the Specification and Implementation Phases in Cryptology'
MJ Toussaint, *Proc. ESORICS 92, pp 77 - 101*

This paper proposes to verify cryptographic protocols by modelling the knowledge states of their participants in an execution tree. As the protocol executes, elements progress from being variables to being fixed, and attacks in progress are revealed by inconsistencies.

5 Secret Key Algorithms

021501 'Generating Bent Sequences'
CM Adams, SE Tavares, *Discrete Applied Mathematics v 39 no 2 pp 155 - 159*

The authors define two classes of bent sequences: a 'bent-based' sequence of order 2^m is a concatenation of 2^{m-2} bent sequences of order 4, and a 'linear-based' sequence is a similar concatenation of linear sequences. They conjecture that all bent sequences fall into one or the other category; this would imply that there are a total of 896 bent sequences of order 16, which has been verified by exhaustive enumeration.

021502 'On the Existence of Periodic Complementary Binary Sequences'
KT Arasu, XA Qing, *Designs Codes and Cryptography v 3 no 2 pp 257 - 262*

A set of periodic complementary binary sequences PCS_p^N is a set of p binary sequences of length N with the property that the sum of all the periodic autocorrelation functions is a delta function. Various conditions on N and p are shown, including that that N must be the sum of two squares and that if $N = p^t u$, $(p, u) = 1$ and $p \equiv 3 \pmod 4$, then $u \geq 2p^{\lfloor t/2 \rfloor}$. It is also shown that there is no PCS_3^{20} or PCS_2^{36}.

021503 'Complete Fibonacci sequences in finite fields'
OJ Brisan, *The Fibonacci Quarterly v 30 no 4 (Nov 92) pp 295 - 303*

Conditions are given under which a finite field has a Fibonacci sequence which spans all its elements or all its squares. Except for $GF(4)$ and $GF(9)$, all these fields are of prime order.

021504 'Linear Nonequivalence versus Nonlinearity'
C Charnes, J Pieprzyk, *Proc Auscrypt 92*

This paper extends the definition of nonlinearity from a Boolean function to a permutation on GF(2^n), and then considers what invariants may be used to establish the linear nonequivalence of two permutations by showing that their coordinates are in different orbits of the affine group acting on the set of Boolean functions on n bits. These invariants include a function's nonlinearity and the Hamming weight of its truth table.

021505 'A VLSI Decomposition of the deBruijn Graph'
O Collins, S Dolinar, R McEliece, F Pollara, *Journal of the ACM v 39 no 4 pp 931 - 948*

The authors show how to construct the deBruijn graph B_n for an n-stage shift register by wiring together many copies of a fixed 'building block' graph. This also gives low cost approximations to B_n, and a number of theorems are proved. Finally, they discuss using this technology in decoding, and extending it to applications such as matrix and polynomial algebra.

021506 'A Hardware Design Model for Cryptographic Algorithms'
J Daemen, R Govaerts, J Vandewalle, *Proc. ESORICS 92, pp 419 - 434*

A design is presented for a high-speed cryptographic processor, named 'Subterranean', which is intended to provide hashing and encryption at Gbit/sec speeds. It is a finite state machine which implements a nonlinear function in GF(2^{256}), the design of which is discussed. This function can be used as the nonlinear feedback function in a self-synchronising stream cipher, as the round function for a block cipher, or as a nonlinear feedback shift register keystream generator.

021507 'Binary Sequences Derived from ML-Sequences over Rings. I: Periods and Minimal Polynomials'
ZD Dai, *Journal of Cryptology v 5 no 3 pp 193 - 207*

The author shows that, given a linear congruential generator over $GF(2^m)$ whose characteristic polynomial is of degree n, one can derive a binary sequence using a class of polynomial functions of the bits of the congruential sequence. She shows that the period of the derived sequence is $2^{m-1}(2^n - 1)$ and provides an upper bound for the linear complexity.

021508 'Cryptanalysis of Summation Generator'
E Dawson, *Proc Auscrypt 92*

This article proposed a divide-and-conquer attack on Rueppel's summation generator - guess one of the shift registers and the carry bit, reconstruct the other, and check for consistency with the target keystream. This is compared with the Meier-Staffelbach attack: the latter works against longer registers but needs a lot more known keystream.

021509 'Constructing Large Cryptographically Strong S-boxes'
J Detombe and S Tavares, *Proc Auscrypt 92*

The authors show how to construct S-boxes using near-bent functions of five variables, and discuss their resistance to differential attack and their static and dynamic independence.

021510 'A High-Speed DES Implementation for Network Applications'
H Eberle, *DEC Systems Research Center report 90*

This report describes a gallium arsenide chip which implements DES in ECB and CBC modes with a throughput of 1Gbit/sec. The techniques used to achieve this are described. The chip is intended for low-latency network controllers, and thus has an efficient key setup mechanism; this in turn makes it cheaper to use in keysearch machines than previously available DES chips.

021511 'A remark on the discrepancy of quadratic congruential pseudorandom numbers'
J Eichenauer-Herrmann, *Journal of Computational & Applied Mathematics v 43 no 3 (Dec 92) pp 383 - 387*

Pairs of numbers from Knuth's congruential pseudorandom number generator may have uniformly good statistical properties, but the same does not hold for k-tuples for any $k \geq 3$. A lower bound is given for the discrepancy of these k-tuples, and it is shown that a positive fraction of such sequences have a k-tuple discrepancy which is an order of magnitude greater than the square root of the modulus.

021512 'Generating a Class of DeBruijn Sequence'
BA Guo, CN Cai, *Proc. Chinacrypt 92 pp 160 - 163*

A class of De Bruijn sequences with large linear complexity can be generated using a cycle joining algorithm of Jansen, and some results about such sequences are given.

021513 'On Primitive and Free Roots in a Finite Field'
D Hachemberger, *Applicable Algebra in Engineering, Communication and Computing v 3 no 2 (1992) pp 139 - 150*

This article investigates the relationship between the additive and multiplicative groups of an extension F_{q^m} of a finite field F_q. It introduces a new family of polynomials, which are additive analogues of the cyclotomic polynomials and can be calculated recursively. These can be used to calculate all primitive and free roots of small field extensions.

021514 'Primitive polynomials over finite fields'
T Hansen, GL Mullen, *Math. Comp v 59 no 200 pp 639 - 643*

The authors extend previous tables by providing a primitive polynomial of degree n, with a minimal number of nonzero coefficients, over the finite field with p elements, where $p \leq 97$ and $p^n < 10^{50}$. They conjecture that (except in a small number of cases) there exists a primitive polynomial whose ith coefficient is a, for all $a \in GF(p)$, all $n \geq 2$ and all i such that $0 \leq i < n$.

021515 'Probabilistic Verification of Boolean Functions'
J Jain, JA Abraham, *Formal Methods in System Design v 1 (1992) pp 61 - 115*

The equivalence of two Boolean functions can be verified by hashing: an integer valued transformation of such functions is presented which is unlikely to produce collisions for inequivalent functions. This is proposed as a technique for verifying designs against formal specifications.

021516 'The Vulnerability of Geometric Sequences Based on Fields of Odd Characteristic'
A Klapper, *Proc Auscrypt 92*

When a binary sequence has been derived from a sequence over a field of odd characteristic q, it is possible to find q from the imbalance in short subsequences. Although the linear complexity of such sequences over GF(2) may be quite high, it is a lot less over GF(q) and an explicit upper bound is derived. A secure sequence must have high complexity with respect to all small primes.

021517 'Cascaded GMW Sequences'
A Klapper, AH Chan, M Goresky, *IEEE Transactions on Information Theory v 39 no 1 (1993) pp 117 - 183*

The binary sequences of Gordon, Mills and Welch have good autocorrelation properties but would need higher linear complexity to be useful in cryptography. By cascading them , the complexity can be suitably increased; the resulting sequences are balanced, have a low, three-valued cross-correlation and can be generated using shift register hardware.

021518 'Cryptanalysis of LOKI91'
LR Knudsen, *Proc Auscrypt 92*

This paper applies differential cryptanalysis to LOKI91 without success, but shows that there is a weakness in the key scheduling which allows an attack with a large number of chosen plaintexts to succeed slightly faster than keysearch would.

021519 'How to predict congruential generators'
H Krawczyk, *Journal of Algorithms v 13 no 4 (1992) pp 527 - 545*

Given integer valued functions ϕ_j, any sequence generated by $s_i = \sum_{j+1}^{k} \alpha_j \phi_j(s_0, ...s_{n-1})$ is efficiently predictable; that is, an attacker who has access to the sequence can recover α_j and m and thus predict it. This improves on previous methods in that, provided only that the ϕ_j are computable in polynomial time, the attacker will take time (and make prediction mistakes) which are polynomial in k and log m. It proceeds by solving a system of equations over the rational numbers to get a multiple of m, and then refining this.

021520 'A Fast Cryptographic Checksum Algorithm Based on Stream Ciphers'
XJ Lai, RA Rueppel, J Woolven, *Proc Auscrypt 92*

The authors propose calculating a keyed checksum of a message by using a keystream to demultiplex the message into two bitstreams, which are then accumulated in two feedback shift registers.

021521 'Continued fraction tactics for cryptanalysis'
DX Li, DW Li, *Chinese Journal of Electronics v 14 no 2 (92) pp 113 - 119*

This paper discusses the application to cryptanalysis of continued fraction techniques based on a theorem of Legendre.

021522 'Polynomial Representation of Periodic Sequence and Fast Determination of Its Complexity'
XD Lin, ZM Hu, CN Cai, *Proc. Chinacrypt 92 pp 148 - 154*

The generalised Boolean polynomial representation of a periodic binary sequence is investigated, and a method of determining this from the sequence is proposed. This leads to a fast algorithm for finding the linear complexity of a binary sequence whose period is divisible by a large power of 2.

021523 'Synthesis of Sequences and Its Applications'
PZ Luo, JJ Zhou, GW Song, *Proc. Chinacrypt 92 pp 140 - 147*

The sequence synthesis problem is described in terms of linear homogeneous equations with polynomial coefficients, which allows a natural generalisation to the nonlinear case. The theory of Gröbner bases in polynomial rings provides an efficient algorithm, which turns out to be a generalisation of Euclid's algorithm, and can deduce an efficient decoding for a class of algebraic codes constructed by Justesen.

021524 'The Period and Linear Complexity of the Output Sequence of a Finite State Machine'
YB Ma, *Proc. Chinacrypt 92 pp 115 - 121*

Every finite state machine sequence combiner whose output function is the sum of N sequence inputs and an internal state variable is correlation immune of order $N-1$, which is the highest possible, and the period of the output sequence can be calculated. Determining the linear complexity is a harder problem, which can be solved in special cases.

021525 'An Approach to the Initial State Reconstruction of a Clock-Controlled Shift Register Based on a Novel Distance Measure'
MJ Mihaljevič, *Proc Auscrypt 92*

A new metric between binary sequences is proposed: if in order to find M bits of sequence A by decimation, one needs to start off with $M + l$ bits of sequence B, then l is taken as the distance between them. Using this 'metric' instead of the Levenshtein distance to attack a clock-controlled shift register sequence gives less false positives; but it still requires $O(2^L)$ calculations to reconstruct the initial state of a shift register of L bits.

021526 'Perfect staircase profile of linear complexity for finite sequences'
M Morii, M Kasahara, *Information Processing Letters v 44 no 2 (Nov 92) pp 85 - 90*

The authors expand the generating function of Rueppel's sequence (which has $s_i = 1$ for $i = 2^j$ and 0 otherwise) as a continued fraction, and show that similar continued fractions give rise to other sequences with staircase complexity profiles. They also calculate the density of the Imamura Yoshida Morii sequence in terms of Fibonacci sequences.

021527 'A Generalised Description of DES-based and Benes-based Permutation Generators'
M Portz, *Proc Auscrypt 92*

Permutation generators based on DES and on Benes networks are special cases of generators based on a Clos network, which is a crossbar switching arrangement which allows arbitrary permutations to be implemented.

021528 'On the power of memory in the design of collision resistant hash functions'
B Preneel, R Govaerts, J Vandewalle, *Proc Auscrypt 92*

A scheme is presented to construct a hash function with a large block size from a block cipher with a smaller block size. A number of block encryptions are performed in parallel, followed by a permutation. A number of possible birthday attacks are analysed, and the tradeoffs between security, memory and speed are discussed.

021529 'The Structure of Families of Linear Recurring Sequences and the Properties of Sum Sequences in $Z/(p^e)$'
WF Qi, JJ Zhou, *Proc. Chinacrypt 92 pp 132 - 139*

Let $G(f(x))$ be the set of all sequences in $Z/(p^e)$ with characteristic polynomial $f(x)$; this can be considered as a $Z/(p^e)$-module or as a $Z/(p^e)[x]$-module. The structure of $G(f(x)) + G(g(x))$ and $G(f(x)) \cap (g(x))$ are described, and used to study the linear complexity and characteristic polynomial of the summation sequence generator.

021530 'Methods for detection of some properties of multiple-valued functions'
RS Stankovič, C Moraga, *IEE Transactions in Computers and Digital Techniques (E) v 139 no 5 (Sep 92) pp 421 - 9*

The authors consider the problem of detecting symmetry in two of the variables of a Boolean function (and, in general, a function over a finite field), and whether such a function can be decomposed. Algorithms are presented and discussed in the context of switching theory.

021531 'The Structure and Property of YC-Sequences'
DF Sun, *Proc. Chinacrypt 92 pp 122 - 131*

YC-sequences are a kind of self-multiplexed sequence constructed in the following way. Let (a_i) be an m-sequence of degree L over $GF(2^m)$ in which g is a primitive element, and let T be a positive integer such that $2^T < L$. Then the YC-sequence will be (b_i) such that $b_i = a_{i+t}$ where $a_{i+2^T} = g^s$ and $s \equiv t \pmod{2^T}$, and $b_i = a_i$ where $a_{i+2^T} = 0$. Such sequences have a period of 2^{mL}-1, in which each nonzero element appears $2^{m(L-1)}$-1 times and zero appears $2^{m(L-1)}$ times. Furthermore, their linear complexity is $L((L+1)^m - 1)$ or $L((L+1)^m - 2)$.

021532 'Message Authentication with One-Way Hash Functions'
G Tsudik, *Computer Communications Review v 22 no 5 pp 29 - 38*

This article proposes basing message authentication on hash functions, in order to get round the hardware cost, software speed and export control problems associated with encryption. The proposed schemes involve using MD4 with a secret prefix or suffix. The latter are more vulnerable to birthday attack.

021533 'Algorithms for Solving Permutation Equations'
JE Wang, *Proc. Chinacrypt 92 pp 186 - 194*

Two new algorithms are presented. The first, given a permutation group G of degree n, can generate a transversal of all right cosets of G in S_n by constructing a reduced representation of G. The second can determine whether an incomplete permutation belongs to a given conjugacy class in S_n.

021534 'Study of some stream ciphers using generating functions'
CK Wu, *Chinese Journal of Electronics v 14 no 5 (92) pp 472 - 478*

Several kinds of stream ciphers - complement sequences, partial sum sequences, inverse order sequences and finitely generated sequences - are studied using generating function techniques. The linear complexity profiles of related finitely generated sequences are also discussed.

021535 'Investigations on DES Transformative Tables II - An Introductory Approach by Permutation Groups'
MZ Xu, *Proc. Chinacrypt 92 pp 181 - 185*

S-boxes are balanced surjective functions which transform n-bit input vectors into m-bit output vectors. Let F be the set of all such functions; then any permutation group S which acts on it will induce a partition $\overline{F} = \{F(f^x) | x \in N_f \setminus S\}$, and all the functions in each equivalence class will have almost the same cryptographic properties. This effectively reduces the study of (S, F) to that of $(S, \overline{F})$, which is a purely pointed permutation group. The structure of N_f is determined in terms of a wreath product.

021536 'On the Enumeration of Boolean Functions Used in Stream Ciphers'
YZ Yang, ZM Hu, *Journal of the China Institute of Communications v 13 no 4 (92) pp 18 - 24*

This paper proves a number of enumeration results about the Boolean functions commonly used in stream cipher systems.

021537 'Construction of an m-ary de Bruijn Sequence'
JH Yang, ZD Dai, *Proc Auscrypt 92*

Maximum length nonlinear shift register sequences of degree m over Z_n are constructed by starting off with an arbitrary feedback function and joining up its cycles. This provides more sequences than previous methods.

021538 'Research on a self-synchronising error-correcting cryptosystem with authentication'
HL Zhang, YM Wang, *Jopurnal of Xidian University v 19 no 3 (92) pp 11 - 18*

This paper presents a self-synchronising error-correcting encryption scheme which can be used to implement authentication. This scheme is shown to have desirable security and reliability properties.

021539 'Highly nonlinear 0-1 balanced Boolean functions satisfying strict avalanche criterion'
XM Zhang, J Seberry, *Proc Auscrypt 92*

This article shows how to construct balanced Boolean functions on n bits which satisfy the strict avalanche criterion and whose minimum distance from any affine function is almost that of a bent function (in fact 2^{n-1} - $2^{\lfloor \frac{n}{2} \rfloor}$). This is done by balancing a bent function on $n-1$ bits.

021540 'HAVAL - A One-Way Hashing Algorithm with Variable Length of Output'
YL Zheng, J Pieprzyk, J Seberry, *Proc Auscrypt 92*

The authors present a hashing algorithm which is based on iterating a round function constructed from applying almost bent functions and shuffling operations on 32-bit words. This may run faster than existing hash functions and its output length can be selected.

021541 'The Extension of Walsh Transform and Nonlinear Approximation of Boolean Functions'
JJ Zhou, WH Chen, *Proc. Chinacrypt 92 pp 216 - 221*

The Walsh transform is extended and used to derive some¡ properties of correlation immunity. A method is shown of finding the best m-th degree approximation to a Boolean function.

021542 'A New Design for Multiplication over Finite Fields'
JY Zhu, ZM Hu, *Proc. Chinacrypt 92 pp 231 - 234*

A multiplier for GF(2^m) is described which uses a polynomial basis representation. The speed depends on the irreducible polynomial chosen to generate the field, and the optimum choice of polynomial is discussed.

021543 'The Homogeneous Complexity of Degree k of De Bruijn Sequences'
SX Zhu, *Proc. Chinacrypt 92 pp 155 - 160*

This paper generalises the linear complexity and quadratic complexity of a De Bruijn sequence s to the homogeneous complexity of degree k, $C_k(s)$. It shows that if s is a De Bruijn sequence of order $n > 3$, and $2 \leq k \leq n-2$, then $C_k(s) \leq 2^n - (C_n^1 + C_n^2 + \cdots + C_n^k)$ -1, and that $C_n(s) = n$+1.

6 Public Key Algorithms

021601 'An efficient public key distribution system'
N Alexandris, M Burmester, V Chrissikopoulos, *Proc IFIP 92 pp 532 - 539*

The authors propose variants of the Okamoto-Tanaka identity-based scheme in which the participants choose their own secret keys (and publish their public keys in a file). The result is a two-way, one-round key exchange protocol with built in authentication.

021602 'A Classification of Algorithms for Multiplying Polynomials of Small Degree over Finite Fields'
A Averbuch, NH Bshouty, M Kaminsky, *Journal of Algorithms v 13 no 4 (1992) pp 527 - 545*

A result of Winograd for infinite fields is extended to show that any algorithm for multiplying together two polynomials of degree n over $GF(q)$ for $q \leq n$, which is optimal, must be based on the Chinese Remainder Theorem.

021603 'How to break a "secure" oblivious transfer protocol'
D Beaver, *Proc Eurocrypt 92*

A security flaw in den Boer's oblivious transfer protocol is described. If the protocol is executed twice, with feedback the second time, the protocol leaks information about the first execution. As this protocol is secure under a zero-knowledge based definition of oblivious transfer, a new definition is proposed and the protocol is adapted to be secure with respect to this new definition.

021604 'Zero-knowledge based identification: from a theoretical concept towards a practical token'
M Burmester, Y Desmedt, *Proc IFIP 92 pp 479 - 485*

This article surveys five available zero-knowledge identification and compares their computational and communications complexity. It discusses ways of dealing with various versions of the middleperson attack and the practicality of implementing one of these schemes in a smartcard.

021605 'Two new types of cryptosystem over Eisenstein's ring $Z[\omega]$'
ZF Cao, *Chinese Journal of Electronics v 14 no 3 (92) pp 286 - 290*

A new type of public key cryptosystem and a new type of ID-based authentication system over Eisenstein's ring $Z[\omega]$ are presented. The security of these two systems depends on the difficulty of integer factoring and logarithmic computation in $Z[\omega]$.

021606 'Threshold Schemes with disenrollment'
AH Chan, B Blakley, GR Blakley, JL Massey, *Proc Crypto 92*

Threshold schemes that allow shares to be compromised and secret keys to be updated by public broadcast are discussed. It is proved that the size of the shares must be at least $L+1$ times larger than the key space in order to allow L shareholders to become compromised. Two schemes that achieve the lower bound are discussed.

021607 'The Design of a Conference Key Distribution System'
CC Chang, TC Wu, CP Chen, *Proc Auscrypt 92*

The authors propose a key distribution scheme which is based on Diffie-Hellman but which incorporates authentication as follows. Let g be a generator mod p, and let each user U_i have a secret key x_i and public key $y_i = g^{x_i}$. In order to communicate with U_j, U_i chooses a random number r, calculates a shared session key $k = y_j^r$, and sends U_j the pair $(g^r, g^{x_i/k})$. U_j can form k as $1/(g^r)^{x_j}$ and check that it was sent by U_i by calculating $y_i^{1/k}$. This scheme has the advantage that it can be extended easily to a conference key scheme.

021608 'Invertibility of Quasi-Linear Finite Automata'
SH Chen, RJ Tao, *Proc. Chinacrypt 92 pp 77 - 86*

A τ-quasi linear finite automaton is defined as a finite order memory nonlinear automaton which depends linearly on the last τ inputs, and the invertibility of such automata is characterised. They can be used to construct public key cryptosystems.

021609 'Threshold Cryptography'
Y Desmedt, *Proc Auscrypt 92*

Threshold cryptosystems are reviewed: they allow decryption or signature to be carried out by k-out-of-l shareholders without the whole secret key having to be reconstituted in the hands of any one person or device. They are suitable for a number of applications, including signatures by organisations and controlling court-ordered wiretaps. Previous schemes had used the Lagrange interpolation formula to find a k numbers whose product is an RSA secret key; it turns out that these schemes can be made provably as secure as RSA by working in a suitable cyclotomic extension of Z_n.

021610 'Non-existence of homomorphic general sharing schemes for some key spaces'
Y Frankel, Y Desmedt, M Burmester, *Proc Crypto 92*

In finite sharing schemes the sets from which one chooses and from which keys are chosen are finite. It is proved that no finite homomorphic sharing schemes exist when the key space is a non-Abelian group (except for particular access structures). The result is generalized to finite fields and Boolean Algebras.

021611 'A Practical Secret Voting Scheme for Large Scale Elections'
A Fujioka, T Okamoto, K Ohta, *Proc Auscrypt 92*

This article reviews previous protocols for electronic voting systems and their known weaknesses. It proposes a new scheme in which each voter passes an encrypted ballot to an administrator, who signs it as evidence of the voter's eligibility; he then passes it to a counter who publishes a list of all the eligible ballots received; and then send his key anonymously to the counter so that his ballot may be opened and counted. Under suitable assumptions about the encryption functions, this scheme can be shown to be sound, private, verifiable and resistant even to collusion between the administrator and the counter.

021612 'Interactive Bi-proof Systems and Undeniable Signature Schemes'
A Fujioka, T Okamoto, K Ohta, *IEICE Trans. Inf. & Syst., v E75-D, no 1 (1992), pp 102–109*

. This paper proposes a new undeniable signature scheme, the 'minimum knowledge undeniable signature scheme', which solves one problem inherent in Chaum's undeniable schemes. The latter consist of two parts, a confirmation protocol and a disavowal protocol. The new scheme proposed in this paper simplifies this by assuring both signature confirmation and disavowal with the same protocol. The construction involves a new proof system, the minimum knowledge interactive bi-proof system, which is shows to exist for every common witness problem. Based on this, a practical construction for undeniable signature schemes is proposed.

021613 'A Practical Digital Multisignature Scheme Based on Discrete Logarithms'
T Hardjono, YL Zheng, *Proc Auscrypt 92*

This paper presents a modified El-Gamal signature scheme which facilitates a notary's certifying that all designated signatories of a document have in fact signed it, and which is secure against adaptive chosen ciphertext attacks.

021614 'Group-Oriented Undeniable Signature Schemes without the Assistance of a Mutually Trusted Party'
L Harn, SB Yang, *Proc. Auscrypt 92,*

The authors combine group-oriented cryptography and undeniable signatures in a scheme where each group member chooses his own secret, and the group public key is determined by all the members. The scheme may be set up to allow a signature to be generated by one member or by all of them; but all members must cooperate to verify a signature.

021615 'Low complexity architecture for exponentiation in $GF(2^m)$'
MA Hasan, VK Bhargava, *Electronic Letters v 28 no 21 (Oct 92) p 1984 - 1986*

The authors present a design for a bit serial multiplier in $GF(2^m)$, which provides efficiency gains by organising the partial products in a neater way. It uses about m^2 clock cycles, needs relatively few components and is particularly suited to exponentiation.

021616 'Efficient ID-based key distribution with tamperfree devices'
T Hwang, *Information Processing Letters v 44 no 1 (Nov 92) pp 31 - 34*

This paper develops the Desmedt-Quisquater idea of using tamperproof devices to implement an identity based key distribution system. Their variant has a number of master keys, of which each user is assigned a subset, and is therefore resistant to the compromise of any single device.

021617 'Elliptic Curve Cryptosystems and Their Applications'
K Koyama, T Okamoto, *IEICE Trans. Inf. & Syst., v E75-D no 1 (1992), pp 50–57*

The authors propose two types of public-key schemes based on elliptic curves modulo n, where n is composite. The paper proposes algorithms for calculating $T = e.S$ over such curves, and uses these to develop two public-key schemes, which are analogues of RSA and Rabin encryption. The former has an encryption function with an odd multiplier, while the latter uses a multiplier of 2. Their security is based on the difficulty of factoring n. Other security characteristics and applications to blind signature are also discussed.

021618 'Secure Addition Sequence and Its Applications on the Server Aided Secret Computation Protocols' CS Laih, SM Yen, *Proc Auscrypt 92*

The authors examine the circumstances in which a server-aided computation protocol can incorporate addition chains without these leaking information on the secret key.

021619 'A Software Implementation for Finite Automaton Public Key Cryptosystem and Digital Signatures'
JB Li, XA Gao, *Proc. Chinacrypt 92 pp 110 - 114*

This paper describes a software implementation of a finite automaton cryptosystem for 80x86 processors. On an 80286 running at 6MHz, unoptimised code achieves speeds of 2766 bps for encryption and 2511 bps for decryption.

021620 'A review of two algebraic-code public key cryptosystems'
YX Li, J Cheng, *Journal of Xidian University v 19 no 1 (92) pp 106 - 111*

This paper outlines two important public key cryptosystems based on algebraic coding theory, namely McEliece's and Niederreiter's. It analyses the two systems and points out some remaining problems and some important applications of coding theory to cryptography.

021621 'Some Notes on McEliece-Sarwate's Secret Sharing Threshold Schemes'
YX Li, XM Wang, *Journal of the China Institute of Communications v 13 no 2 (92) pp 92 - 93*

This paper examines the two schemes of McEliece and Sarwate, MSTS1 and MSTS2. It is shows that MSTS1 is insecure, while MSTS2 is not in fact a (k, n) threshold scheme, but a $(1, k, n)$ ramp scheme.

021622 'On the Security of Niederreiter's Public Key Algebraic-Code Cryptosystem and the Optimization of Parameters'
YX Li, XM Wang, J Cheng, *Proc. Chinacrypt 92 pp 59 - 65*

In this paper, the security of Niederreiter's public key system is analysed, and a new attack method using linear algebra is given. It is shown that Niederreiter's system has the same security as McEliece's. Finally, the security parameters of the two systems are compared.

021623 'Modified Maurer-Yacobi's scheme and its applications'
CH Liu, PJ Lee, *Proc Auscrypt 92*

This paper discusses certain weaknesses with the Maurer-Yacobi scheme, and a number of variants for signature and key distribution. However, experiments with the Pohlig-Hellman algorithm indicate that such schemes take 30-150 hours to compute each member's secret key on a typical workstation, which casts doubt on their practicality.

021624 'ID-Based Public Key Cryptosystems with Direct Authentication and Reliable Signature'
LR Lu, RJ Zhao, *Proc. Chinacrypt 92 pp 40 - 48*

The security of the Tsai-Hwang ID-based scheme can be compromised without solving the underlying factoring and discrete log problems. Two modified schemes are presented which resist this attack and offer reliable authentication and signature.

021625 'Algebraic Properties of Cryptosystem PGM'
SS Magliveras, ND Memon, *Journal of Cryptology v 5 no 3 pp 167 - 183*

The authors show that the cryptosystem PGM is not closed under functional composition, that some multiple encryption will map any k distinct plaintexts to any k distinct ciphertexts, and (provided the underlying group is not abelian or hamiltonian, and its order is not equal to a power of 2 or to the order of any finite simple group) that its transformations generate the full symmetric group.

021626 'On Verifiable Implicit Asking Protocols for RSA Computation'
T Matsumoto, H Imai, CS Laih, SM Yen, *Proc Auscrypt 92*

This paper considers ways of preventing attacks on server-aided computation protocols, and, in particular, proposes to block the Pfitzmann-Waidner passive attack by splitting the server computation into two phases.

021627 'Group-oriented key Management and Authentication Method'
Y Mutoh, K Takagi, KI Okada, Y Matsushita, *Proc IFIP 92 pp 540 - 546*

The authors discuss group-oriented systems where each user holds a piece of a group key and some pieces unique to himself. Combinatorial techniques are to be used to generate communication keys from any r cooperating users.

021628 'Number Characterisation and Irrepetitious Enumeration for $GL_n(GF(q))$'
ZP Qin, HG Zhang, *Proc. Chinacrypt 92 pp 204 - 208*

A procedure for generating random matrices is proposed which can be of assistance when implementing the finite automaton and McEliece public key schemes.

021629 'New Public-Key Cryptosystem Based on Factorisations of Finite Groups'
MH Qu, SA Vanstone, *Proc. Auscrypt 92,*

A generalised knapsack scheme is presented which is based on factorisation of a finite group, ie a collection of subsets A_i of a group G such that each $g \in G$ can be represented as $\prod a_i$ where $a_i \in A_i$.

021630 'Subliminal channels for signature transfer and their application to signature distribution schemes'
K Sakurai, T Itoh, *Proc Auscrypt 92*

The parallel version of Fiat-Shamir has an extra subliminal channel. This can be used to implement distributed threshold verification. A distributed signature scheme is defined as one which requires the cooperation of all verifiers in order for the signature to be published.

021631 'On the Identity-Based Key Exchange Protocols'
M Shafa'amry, M Scott, *Dublin City University report CA-2592*

This report describes the identity-based key exchange schemes of Okamoto, Girault, Maurer-Yacobi, Günter, Bauspieß-Knobloch and Okamoto-Ohta, and compares their secret key size, computation requirements and communication overhead (including whether they are interactive or not). It also reports a PC implementation of the Maurer-Yacobi scheme.

021632 'Lyndon Trees'
KG Subramanian, R Siromoney, L Mathew, *Theoretical Computer Science v 106 (92) p 373 - 383*

This paper introduces the concept of Lyndon trees. These are trees which are strictly less than any of their conjugates. Their properties are investigated, and the authors develop a public key cryptosystem based on them which extends one of the authors' earlier work on cryptosystems based on Lyndon words.

021633 'An Implementation of Identity-Based Cryptosystems and Signature Schemes by Finite Automaton Public Key Cryptosystems'
RJ Tao, SH Chen, *Proc. Chinacrypt 92 pp 87 - 104*

This paper presents indentity-based key distribution and signature schemes based on the invertibility theory of finite automata, which can resist collusion attacks.

021634 'Cryptanalysis of the Xinmei digital signature scheme'
J van Tilburg, *Electronics Letters v 28 no 20 (92) p 1935 - 6*

This note shows how to break the Xinmei digital signature scheme, as well as a variant by Harn and Wang, by recovering the secret matrix from the public key information in each case.

021635 'An RSA based public-key cryptosystem for secure communication'
VCH Venkaiah, *Proc Indian Academy of Science, v 102(2) (August 1992), pp 147–153*

This paper presents a new system based on RSA. One advantage is that the encryption and decryption procedures are computationally less intensive. An illustrative example is given and some possible attacks are considered.

021636 'The Probability Distribution of the Diffie-Hellman Key'
CP Waldvogel, JL Massey, *Proc Auscrypt 92*

When g is a generator of Z_p^*, and both A and B are chosen at random in Z_{p-1}, then the probability distribution of g^{AB} is closest to uniform where $p-1=2q$ for q prime, and furthest from uniform when $p-1$ is smooth. In the former case, the ratio of the probabilities of the most and least likely keys is about 6, while in the latter it is about 10^{12} for a 100-digit modulus p. Thus primes which are secure with respect to the Pohlig-Hellman algorithm are also secure with respect to the key probability distribution.

021637 'Performance Analysis and Parameter Optimisation on the M-public-key Cryptosystem'
YM Wang, HL Zhang, *Acta Electronica Sinica v 20 no 4 (92) pp 32 - 36*

In this paper, a formula is derived for the error-correcting performance of the generalised M-public-key cryptosystem. The trade-off between the parameters t and $W(Z)$, the security and the error-correcting performance is discussed and an approach to optimising the parameters is given.

021638 'Comments on the Security of Pieprzyk Public Key Cryptosystem and on Yang Attack Method'
DQ Xie, *Proc. Chinacrypt 92 pp 16 - 19*

It is pointed out that Yang's attack on the Pieprzyk public key cryptosystem is a partial attack; an instance is given which cannot be attacked by this method. A new attack is shown which works against all instances so long as deg $p_i(x)a(x)$ <deg$v(x)$.

021639 'More about the active attack on the server-aided secret computation protocol'

SM Yen, CS Laih, *Electronic Letters v 28 no 24 (Nov 92) p 2250*

In response to Anderson's one-round active attack on server-aided computation protocols, the authors propose that the calculation be blinded; the message to be signed should be multiplied by a random number R, and the resulting signature divided by R^e, where e is the signer's secret key.

021640 'The Fast Cascade Exponentiation Algorithm and Its Application to Cryptography'

SM Yen, CS Laih, *Proc Auscrypt 92*

The authors consider the use of addition chains to speed up the computation of $M_1^{b_1} M_2^{b_2} M_3^{b_3} \pmod{n}$, which provides an improvement of 20% or so over existing methods.

021641 'Implementation of FA Public Key Cryptosystem'

HG Zhang, DW Dai, ZP Qin, K Wu, BQ Cui, H Han, *Proc. Chinacrypt 92 pp 105 - 109*

This paper describes an implementation of the finite automaton public key cryptosystem on a microcomputer. Encryption and decryption turn out to be faster than with RSA.

021642 'MC-Veiled Lower Transform Public Key Cryptosystem'

BD Zheng, *Acta Electronica Sinica v 20 no 4 (92) pp 21 - 24*

This paper presents a new type of public key cryptosystem, the security of which largely depends on the matrix cover problem.

7 Computational Number Theory

021701 'Irregular primes to one million'
JP Buhler, RE Crandall and RW Sompolski, *Math. Comp v 59 no 200 pp 717 - 722*
The authors compute all irregular primes up to one million, along with the index of the associated Bernoulli number.

021702 'Steiner triple systems of order 19 with nontrivial automorphism group'
CJ Colbourn, SS Magliveras and DR Stinson, *Math. Comp. v 59 no 199 pp 283 - 295*
Even for small orders, Steiner triple systems are too numerous for exhaustive enumeration. The authors show that if the restriction of a nontrivial automorphism group is imposed, then there are 172,248 such systems of order 19.

021703 'Prime Generation with the Demytko-Miller-Trbovich Algorithm'
L Condie, *Proc Auscrypt 92*
This paper reports experimental work in which about 10^6 primes were generated from smaller primes by testing $p_{k+1} = hp_k + 1$ for primality using small random values of h. The output appeared random, and after two such steps even the number of digits in the output primes was unpredictable.

021704 'Generating M-strong Fibonacci pseudoprimes'
A Di Porto, P Filipponi, *The Fibonacci Quarterly v 30 no 4 (Nov 92) pp 339 - 343*
A composite number is called an M-strong Fibonacci pseudoprime if it passes the Lucas test for indices 1 through M. The authors derive conditions for this and show how to generate such numbers.

021705 'On the normal growth of prime factors of integers'
I Kátai, A Mercier, *Canadian Journal of Mathematics v 44 no 6 (Dec 92) pp 1121 - 1154*
This paper considers the number of prime divisors of a number n using Erdős' function $T(n,y) = \sum_{q|n,q<y} h(\frac{log q}{log y})$, where h belongs to a large class of functions, and in particular investigate the number of divisors of n such that $T(n,y) < z$.

021706 'On Strong Dickson Pseudoprimes'
G Kowol, *Applicable Algebra in Engineering, Communication and Computing v 3 no 2 (1992) pp 129 - 138*
A composite integer n is called a strong Dickson pseudoprime (SDPP) to the parameter c if $g_n(b,c) \equiv b \pmod{n}$ for all b in Z, where $g_n(z,c)$ is the nth Dickson polynomial. This generalises Carmichael numbers, which are exactly the SDPPs for $c = 0$, and include the SDPPs with c=-1. It is shown here that n is a SDPP to the parameter c if and only if (1) it is odd and squarefree, and if $n = p_1 p_2 ... p_r$, then for all i (2) $ord_{p_i}(p_i + 1)$ divides $n - 1$ or $n(p_i)$ and (3) if $c \neq 1 \pmod{p_i}$, then $(p_i - 1)$ divides $(n - 1)$; otherwise it divides either $(n - 1)$ or $(n + 1)$. It follows that if n is a SDPP to the parameter c for $\gcd(c, n)$=1, then it is also one to the parameter 1.

021707 'An Efficient Block-Oriented Approach to Sparse Choleski Factorisation'
E Rothberg, A Gupta, *Stanford University report STAN-CS-92-1438*
This report discusses strategies for decomposing a large sparse binary matrix into rectangular blocks. This has considerable potential advantages over column methods on parallel machines; some experimental results are given.

021708 'Probabilistic Distribution of the Rank of a Random Matrix over F_2'
JM Sheng, MQ Huang, *Proc. Chinacrypt 92 pp 195 - 198*
This paper investigates the probabilistic properties of the rank of a random k by n binary matrix. The asymptotic properties of this for two significant cases are discussed.

021709 'Optimal Algorithms for multiplication in certain finite fields using elliptic curves'

MA Shokrollahi, *SIAM Journal of Computing v 21 no 6 (Dec 92) pp 1193 - 1198*

Multiplication in $GF(q^n)$ has bilinear complexity $2n$ where n is within about $\sqrt{q}$ of $\frac{1}{2}q + \sqrt{q}$. This is achieved by means of Lagrange interpolation on a suitable elliptic curve.

021710 'The distribution of safe primes and strong primes'

W Wang, *Proc. Chinacrypt 92 pp 172 - 180*

This paper discusses the distribution of primes p such that $p - 1$ has a large prime factor. Various estimates, including upper and lower bounds for the number of these primes, are given.

021711 'Weight formulas for ternary Melas codes'

G van der Geer, R Schoof and M van der Vlugt, *Math. Comp v 58 no 198 pp 781 - 792*

By specializing some of their earlier work, the authors derive a formula for the frequencies of the weights in ternary Melas codes and give a table of weight frequencies.

8 Theoretical Cryptology

021801 'Multiparty Protocols, Pseudorandom Generators for Logspace, and Time-Space Trade-Offs'
L Babai, N Nisan, M Szegedy, *Journal of Computer and System Sciences v 45 no 2 (92) pp 204 - 232*

The authors define the generalised inner product, GIP_k, of k n-bit strings to be the parity of their bitwise AND. This is useful in two ways: firstly, an upper bound is proved on its discrepancy over cylinder intersection sets, which leads in turn to a lower bound on the communication complexity of evaluating an arbitrary Boolean function; and secondly, that as this function requires $O(n)$ steps to evaluate on a k-head Turing machine and $O(n^2)$ on a $(k-1)$-head machine, it follows that 'more heads are better'. It also follows that two-way access to random bits is better than one-way access.

021802 'Uniform results in polynomial-time security'
P Barbaroux, *Proc Eurocrypt 92*

A general framework is considered in which classical sampling techniques can be applied to obtain uniform results. Most security results can be established in both a uniform and a non-uniform model of computation. The main theorem gives sufficient conditions for extending non-uniform results to uniform ones. From this, as a consequence, the uniform version of Schrift and Shamir's generalisation of Yao's theorem on the universality of the next bit test is derived.

021803 'Tools for proving zero-knowledge'
I Biehl, J Buchmannn, B Meyer, C Thiel, C Thiel, *Proc Eurocrypt 92*

The authors discuss a general technique for proving the zero-knowledge property of interactive zero-knowledge proofs. The approach is theoretical and is based on an analysis of probabilistic Turing machines whose outputs are circuit indistinguishable.

021804 'Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes'
EF Brickell, DR Stinson, *Journal of Cryptology v 5 no 3 pp 153 - 166*

The authors provide an introduction to secret sharing schemes, and prove that any graph of maximum degree d has a perfect scheme whose information rate is at least $d+3$. The proof involves constructing perfect schemes on graphs composed of small graphs which already have such schemes.

021805 'Universally Secret Sharing Schemes'
B Chor, A Beimel, *Crypto 92*

In ideal sharing schemes the size of the shares is identical to the size of the key and in universally ideal ones this is true for all possible sets of keys. It is proved that an access structure is universally ideal if and only if it is ideal for the case that the key set has cardinality 2 and also for the case of cardinality 3. Examples illustrate that each condition alone is not sufficient.

021806 'Non-interactive circuit based proofs and non-interactive perfect zero knowledge with preprocessing'
I Damgård, *Proc Eurocrypt 92*

A non-interactive zero-knowledge proof for SAT is presented. This is based on quadratic residuosity, and is significantly more efficient than earlier proofs. The author also considers non-interactive zero-knowledge arguments. Under a general assumption (that collision intractable hash functions exist), a statistical zero-knowledge non-interactive argument with preprocessing for any NP statement is presented. The length of the preprocessing messages is independent of the size of the theorem to be proved. Under the certified discrete log assumption, the protocol is perfect zero-knowledge.

021807 'On the Information Rate of Secret Sharing Schemes'
A De Santis, C Blundo, L Gargano, U Vaccaro, *Proc Crypto 92*

This paper presents two families of access structures with optimal information rate $1/2+\epsilon$: that is, in any sharing scheme for these access structures there is a shareholder whose shares are roughly twice as long as the secret key. For one of these families, the average optimal information rate is $1/2+\epsilon_k$, where $\lim_{k\to\inf}\epsilon_k = 0$. A family of access structures with optimal information rates bounded above by similar bounds is proved to be NP-complete and lower bounds for families of access structures are presented.

021808 'Perfectly Secure Message Transmission'
D Dolev, C Dwork, O Waarts, M Yung, *Journal of the ACM v 40 no 1 (1/93) pp 17 - 47*

The authors consider the case where two parties have n communications links between them, of which ρ are subject to noise and σ (not necessarily distinct) are subject to surveillance. They show that the parties can communicate with perfect secrecy if and only if $n \geq \sigma+\rho+1$ where the communication is one-way, and $n \geq max\{\sigma+\rho+1, 2\rho+1\}$ where it is two-way. A number of related results are shown, concerning the effects of cooperation between the monitoring and disrupting adversaries and verifiable secret sharing.

021809 'Determinism vs nondeterminism in multiparty communication complexity'
D Dolev, T Feder, *SIAM Journal of Computing v 21 no 5 (Oct 92) pp 885 - 895*

If we have a nondeterministic algorithm which will evaluate a Boolean function f whose input is distributed among a number of players, and which exchanges C_1 bits with k_1 parties when $f=1$ and C_2 bits with k_2 parties when $f=0$, then there is a deterministic algorithm which communicates with $2k_0^2k_1$ parties and exchanges $2[C_1+k_1 log k_0+1][C_0+k_0(log 2k_0^2k_1)+2]$ bits with each of them.

021810 'Low communication 2-prover zero-knowledge proofs for NP'
C Dwork, U Feige, J Kilian, M Naor, M Safra, *Proc Crypto 92*

With multiple-prover interactive proofs, many provers try to prove a theorem to a single verifier; and they can achieve zero-knowledge without having to rely on complexity assumptions, such as the existence of one-way functions. In this paper their communication complexity is considered. A 2-prover perfect zero-knowledge proof for 3-SAT is presented, in which the length of the query that the verifier asks each prover, and the number of random bits they must share, both grow logarithmically in the size of the 3-SAT formula, but the answer of each prover is of constant length. In a single-prover zero-knowledge proof, this is only possible if $NP \subset BPP$; and if this holds, there is a lower bound for the number of shared random bits in the multiple-prover case.

021811 'Finite State Verifiers I: The Power of Interaction'
C Dwork, L Stockmeyer, *Journal of the ACM v 39 no 4 (92) pp 800 - 828*

Where the verifier is a 2-way probabilistic finite state automaton, interactive proof systems with private randomisation are strictly stronger than those with public randomisation, which in turn are strictly stronger than those with no randomisation at all. There is also an interactive proof system for every language which can be recognised in exponential time.

021812 'Finite State Verifiers II: Zero Knowledge'
C Dwork, L Stockmeyer, *Journal of the ACM v 39 no 4 (92) pp 829 - 858*

This is the journal version of the authors' Crypto 88 paper, in which they show that for a verifier which is a 2-way probabilistic finite state automaton, not all languages with interactive proofs have zero knowledge proofs, and if the verifier is also sweeping, then it can check zero knowledge proofs for languages which it cannot recognise in polytime.

021813 'Self-witnessing Polynomial Time Complexity and Prime Factorisation'
MR Fellowes, N Koblitz, *Designs, Codes and Cryptography v 2 no 3 (1992) pp 231 - 235*

The authors call a problem 'P-time self witnessing' if it is has the property that if a polynomial time algorithm exists for it, then we know it this algorithm constructively. This concept has been used implicitly for some 20 years. Factorisation in particular is P-time self-witnessing by Levin's diagonalisation argument, as is k-fold planar cover search. If an NP-hard problem could be shown to have this property, then a nonconstructive proof of $P = NP$ would be impossible.

021814 'The Lempel-Ziv Algorithm and Message Complexity'
EN Gilbert, TT Kadota, *IEEE Transactions on Information Theory v IT-38 no 6 pp 1839 - 42*
The authors address the problem of discriminating between message sources with different characteristics by using Lempel-Ziv compression to estimate complexity; more redundant messages compress more.

021815 'Non-interactive zero-knowledge proofs and invariant signatures are equivalent'
S Goldwasser, R Ostrovsky, *Proc Crypto 92*
A connection is established between two basic primitives: non-interactive zero-knowledge proofs and invariant digital signatures. It is well known that digital signatures can be implemented using any one-way function, whereas non-interactive zero-knowledge proofs with polynomial time users require trapdoor permutations. To make the connection, the concept of invariant digital signatures is introduced. These are signatures with a 'fingerprint' property, for which each document has a unique signature, or at least all signatures of the same document are alike. A formal setting is presented and it is shown that non-interactive zero-knowledge proofs and invariant digital signatures are equivalent primitives.

021816 'An l-Span generalized secret sharing scheme'
L Harn, HY Lin, *Proc Crypto 92*
A conditionally secure general sharing scheme is presented. It has the property that its shareholders can recompute l keys in a given order. If the first j keys have been revealed it is hard to compute the next ones even with the help of shareholders not in the access structure.

021817 'Constructions of Feebly-One-Way Families of Permutations'
APL Hiltgen, *Proc Auscrypt 92*
Families of permutations are exhibited whose minimum circuit complexity tends to half the complexity of their inverses. These are derived from star graphs.

021818 'A comparison of key distribution patterns constructed from circle geometries'
CM O'Keefe, *Proc Auscrypt 92*
Key distribution patterns have previously been based on two of the three circle geometries, namely the inversive and Laguerre planes. This paper constructs them for the third, the Minkowski planes, and compares the performance of the various constructions.

021819 'Cryptographic Hardness of Distribution-Specific Learning'
M Kharitonov, *Stanford University report STAN-CS-92-1445*
This report presents an application of theoretical cryptology: to prove that certain problems in learning theory are intractable. In particular, learning a Boolean function (or a constant-depth circuit) is hard, provided that factoring (or some other problem) is.

021820 'Random Texts Exhibit Zipf's-Law-Like Word Frequency Distribution'
W Li, *IEEE Transactions on Information Theory v IT-38 no 6 pp 1842 - 45*
It is shown that if one generates a random text, it obeys Zipf's law (that the distribution of word frequencies follows an inverse power law). It follows that Zipf's law is not a property of language but of its representation.

021821 'Algebraic Methods for Interactive Proof Systems'
C Lund, L Fortnow, H Karloff, N Nisan, *Journal of the ACM v 39 no 4 (92) pp 859 - 868*

This is the journal version of the authors' FOCS 1990 paper, in which they show that the polynomial hierarchy has an interactive proof by giving such a proof for the permanent of a matrix. This is achieved by reducing the problem to one in a finite field, in which the permanent is a low-degree polynomial.

021822 'Communication Complexity of Secure Distributed Computation in the Presence of Noise'
EH Modiano, A Ephremides, *IEEE Transactions on Information Theory v IT-38 no 4 (92) pp 1193 - 1202*

The authors extend the results of Orlitsky and ElGamal on secure distributed computation to the case where the public channel is noisy, and show that this slightly reduces the number of secret bits required.

021823 'Some Studies on Authentication Codes and Their Construction'
DY Pei, *Proc Chinacrypt 92 pp 66 - 73*

This paper reviews results on authentication achieved by Chinese researchers in recent years, including information-theoretic bounds on the probability of spoofing attacks of order r, and codes constructed using finite geometry and partially balanced incomplete block designs.

021824 'Strongly Ideal Secret Sharing Schemes'
SJ Phillips, NC Phillips, *Journal of Cryptology v 5 no 3 pp 185 - 191*
Strongly ideal secret sharing schemes are those whose set of possible shares is just the set of secrets. The only access structures which can be realised by such schemes are those whose basis is $\{X\}$, $\{\{x\} : x \in X\}$, or $\{\{x, y\} : x \in X, y \in Y\}$ for disjoint subsets X and Y of the population.

021825 'On threshold circuits and polynomial computation'
JH Reif, SR Tate, *SIAM Journal of Computing v 21 no 5 (Oct 92) pp 896 - 908*

All functions which can be computed by threshold circuits whose depth and size are polynomial in n, can also be computed using sums and products in $GF(p)$ where p is polynomial in n (and conversely). Threshold circuits of polynomial size and constant depth can compute a large number of functions, including division, polynomial interpolation and FFT.

021826 'On the discrepancy between serial and parallel zero-knowledge protocols'
K Sakurai, T Itoh, *Proc Crypto 92*

It is known that the parallel versions of interactive zero-knowledge proofs leak partial information. In the case of the parallel version of the Fiat-Shamir proof, this can be used by a dishonest verifier to obtain a signature for any message. The discrepancy between serial and parallel executions of zero-knowledge protocols is investigated in the general case. It is shown that the parallel versions of the Guillou–Quisquater, Okamoto–Ohta and Desmedt authentication schemes can also be attacked in this way. On the other hand, parallel versions of authentication schemes can be used to get transitive traces (for testifiable authentication), while parallel versions of divertable proofs can be used for blind signatures and for protection against middle person attacks.

021827 'On Bit Correlations Among Preimages of "Many to One" One Way Functions'
K Sakurai, T Itoh, *Proc Auscrypt 92*

The authors explore ways of extending the concept of a hard core predicate to collision resistant hash functions. They propose to measure the complexity of such functions by the number of preimages of a hash value which satisfy a given predicate.

021828 'IP = PSPACE'

A Shamir, *Journal of the ACM v 39 no 4 (92) pp 869 - 877*

This is the journal version of the author's famous FOCS 1990 paper, in which he shows that IP = PSPACE. In particular, he provides an interactive proof for quantified Boolean formulae; this is achieved by arithmetising the problem.

021829 'IP = PSPACE: simplified proof'

A Shen, *Journal of the ACM v 39 no 4 (92) pp 878 - 880*

This presents a simplified version of Shamir's IP = PSPACE proof, which uses degree reduction in a suitably large finite field.

021830 'New General Lower Bounds on the Information Rate of Secret Sharing Schemes'

DR Stinson, *Proc Crypto 92*

Let the rank of an access structure be the maximum cardinality of a minimal authorized subset. For access structures of rank two with the number of shareholders less than 6, the existence of several sharing schemes is proven. Other lower bounds for the information rate of other access structures are also provided.

021831 'Measures of Uncertainty and Information in Computation'

JF Traub, H Woźniakowski, *Information Sciences v 65 (92) pp 253 - 273*

The radius of information, $r(N)$, is used in information-based complexity theory to measure the intrinsic uncertainty of a problem and thus give a lower bound on the average error of algorithms in numerical analysis. The authors define the 'value of information', $V(N)$, as $log(\frac{log(N)}{log(0)})$ and give various examples and results.

021832 'Authentication Codes Constructed by Plane Curves'

YJ Wang, *Proc Chinacrypt 92 pp 74 - 76*

For every prime power q and positive integer $k < q - 1$, there is an authentication code with q source states, q^2 messages and $q^k(q-1)$ encoding rules (defined by plane curves), such that for $r \in \{1, 2, ..., k\}$, the probability of a successful spoofing attack achieves the information theoretic bound of $2^{H(E|M^{r+1})-H(E|M^r)}$, which is equal to $1/(q-1)$ if r=1 and $1/q$ otherwise.

9 Book Review

'On the Design and Security of Block Ciphers'

Xuejia Lai
ETH Series in Information Processing, vol 1, 1992 (Hartung-Gorre Verlag, Konstanz)

This is the IDEA book - the book which explains the International Data Encryption Algorithm used in PGP and elsewhere. It may well become the standard work on block ciphers, as it provides the first full worked example of how to design and test such an algorithm.

After a brief introduction to cryptology, IDEA is described and its design principles are explained in detail. It is an eight-round iterated block cipher, with each round made up from three different operations on 16-bit values - bitwise exclusive or, addition modulo 2^{16} and multiplication modulo $2^{16}+1$. These operations are used because they are incompatible; no distributive or generalised associative law holds between any pair of them, and this is described in terms of the theory of algebraic groups. The effect is to make algebraic attacks difficult, and to guarantee good diffusion.

Next, the algorithm's vulnerability to differential cryptanalysis is considered. There is a very clear exposition of how this attack works, and the concept of a Markov cipher is introduced to formalise it. This applies the theory of Markov chains to iterated ciphers, and shows that such ciphers should have an asymmetric transition matrix. It is argued that IDEA should resist any differential attack, and numerical results for miniature versions of it are presented in support.

The book closes with a review of the ways in which such a block cipher can be chained to produce a hash function, and the various attacks possible in each case. All in all, a first-class book which should be in the library of everyone interested in cryptographic algorithms.