Computer and Communications

Security Reviews

Volume 2 Number 2 June 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.

Erratum: The list of contributing editors for the last issue (volume 2, issue 1) omitted Tom Cusick by mistake.

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by 7 May 1992; and books and technical reports received by the editor prior to this date.

We also have reviews of papers presented at the following conferences (including a number of papers from NCSC 92 which were not ready in time for the previous issue). Note that we have started reviewing proceedings which have recently been published, as well as those of conferences which have recently taken place; it does not seem practical to follow either policy strictly.

SPRC 93: proceedings of the 3rd Symposium of State and Progress of Research in Cryptography, Rome, 15-16/2/93 published by Fondazione Ugo Bordoni
Cambridge Workshop: Cambridge Formal Methods Workshop, Cambridge 14-16/4/93 *Proceedings to be published by Cambridge University Computer Laboratory*
Data Compression 93: IEEE Data Compression Conference, 30/3 - 2/4/93, Snowbird, Utah *published by IEEE*
Proc NCSC 92: Proceedings of the 15th National Computer Security Conference, Maryland, USA, 13-16/10/1992, *published by US National Institute of Standards & Technology (US GPO:1992-625-512:60546)*
Physcomp 92: *Workshop on Physics and Computation, 2-4 October 1992, Dallas, Texas* ISBN 0-8186-3420-0
Las Vegas proceedings: *Proceedings of the first international conference on finite fields, coding theory, and advances in communications and computing, Las Vegas, 7-10/8/1991* Lecture notes in pure and applied mathematics v 141, Marcel Dekker (92) ISBN 0-8247-8805-2
Bilkent proceedings: *Bilkent International Conference on New Trends in Communication, Control, and Signal Processing, Ankara, 2-5/7/90* Elsevier, Amsterdam

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

022101 'Retail Banking'
D Austin, *Banking Technology (Dec 92/Jan 93) p 14*

This article reports the 1992 'Technology in Retail Banking' conference and in particular the discussions there of card fraud. There was controversy about the usefulness of expert systems in detecting fraud in progress, due to the low level of online authorisations in the UK and the small proportion of the total number of transactions which result from stolen card use.

022102 'All the smart moves'
D Austin, *Banking Technology (Feb 93) pp 30 - 32*

This article considers why smartcards have not been more widely adopted outside France. UK banks are constrained by the scale of existing investment, worries about costs and general inertia; nonetheless, a working group is currently trying to agree a whether the next generation card should be smartcards, memory cards or watermark cards.

022103 'Spain tops European ATM League'
Banking Automation Bulletin for Europe (Dec 92) pp 1 - 6

During 1992, the number of ATMs in Europe rose past 100,000; this is ahead of the USA but just behind Japan. Spain, with over 18,000, has most; while less developed countries such as Turkey show the fastest growth. The article covers the number of machines by country, their density compared with the population, cash volumes and networking information. By comparison, India and China have only a few dozen machines, although China should be a boom market in future.

022104 'A tamper-resistant seal for trusted distribution and life-cycle integrity assurance'
M Bianco, *Proc NCSC 92 pp 670 - 679*

The author discusses methods available to prevent and detect tampering with hardware. Packaging can be replaced, alarms reset, and seals replaced; as an alternative, an electronic seal is proposed which provides a cryptographically protected audit trail of all accesses, authorised or not, to a hardware enclosure.

022105 'An SDNS platform for trusted products'
E Borgoyne, RG Puga, *Proc NCSC 92 pp 564 - 573*

The authors describe the US government's Secure Data Network System (SDNS) and a platform which allows commercial trusted products to be used with it. This platform, which is based on Trusted XENIX, acts as the SDNS security boundary: its encryption capabilities allow classified data to be sent over unclassified networks, and it has VME busses for both RED and BLACK extension cards. It will typically be configured as a LAN or WAN security server, providing administration, access control and audit functions to a number of users.

022106 'A LAN security primer'
RE Carlson, *Computer Fraud and Security Bulletin (Mar 93) pp 5 - 11*

The author describes Novell's project to get a version of its Netware operating system certified to C2 under TCSEC. The main problem is the intelligent workstation, as a machine running DOS can hold all sorts of programmers' trapdoors; this problem is tackled using special ROMs which limit DOS to the A: drive. Some makes of PC have BIOS loopholes which also need to be stopped up; and passwords are encrypted using an RSA derivative before they are shipped to the server for checking. No other objects need to be encrypted at C2, although fuller encryption can be provided by third party products.

022107 'Objectives and costs in peer entity negotiation'

W Diffie, *SPRC 93 pp 9 - 16*

Most secure sessions start with a negotiation process, whose aim may include session key setup, entity authentication, agreement on classification level, and algorithm selection; the design involves trade-offs with the cost of implementation, computation and communication. This is discussed with reference to secure telephone design: last generation systems used exponential key exchange, with authentication provided either implicitly by voice recognition, or explicitly by a spoken checksum; while the latest ISDN products add automatic authentication and credential exchange, the mechanisms for which are described.

022108 'Practical Quantum Cryptography Based on Two-Photon Interferometry'

AK Ekert, JG Rarity, PR Tapster, GM Palma, *Physics Review Letters v 69 no 9 (31 Aug 1992) pp 1293 - 1295*

This article reports the implementation of quantum cryptography using Mach-Zehnder interferometers. The technique is estimated to have a possible range of 10 - 20 Km.

022109 'European banks gear up for global card system'

Financial Technology International Bulletin v X no 2 (Oct 92) p 1 - 2

The merger of Eurocheque and Eurocard has produced a consortium of European banks, which are launching a debit card system to compete with VISA. Called Edc/Maestro, it will use magnetic strip technology with identification being by either PIN or signature.

022110 'Canadian banks to build large value payments system'

Financial Technology International Bulletin v X no 6 (Feb 93) pp 2 - 3

The Canadian Payments Association are currently studying whether they can extend an existing payment mechanism to cope with large value payments. The objects of study include getting a precise time of finality of payment, and setting debit caps on participants as a function not just of their capital but also of the credit extended to them by other participants.

022111 'Corporates want standard entry into banks' service'

Financial Technology International Bulletin v X no 7 (Mar 93) pp 3 - 4

Differences in banks' EDI interfaces are a problem for their corporate customers, and security is a particular problem. Customers want a single solution covering confidentiality and authentication, and this requirement has been set out in a report by the UK Article Numbering Association.

022112 'Finding Security Flaws in Concurrent and Sequential Designs using Planning Techniques'

DA Fincke, M Archer, K Levitt, *Proc NCSC 92 pp 194 - 203*

The authors describe an automated tool which searches for security flaws by trying to generate sequences of operations which breach the security policy. This tool, called SPLAN, is implemented in Prolog and can utilise domain specific knowledge (such as that covert channels arise in the presence of context switches between processes). It was successful at finding a known flaw in a mutual exclusion algorithm.

022113 'Waiting for Taurus'

J Green-Armitage, *Computer Weekly March 4 1993 pp 28 - 29*

This article describes Taurus, a share transfer and registration system being developed by the International Stock Exchange in London (and which has been cancelled since this article was written). It used IBM's common cryptographic architecture, with PCs at participant sites using encryption cards to implement DES and smartcards for key management, while the central site had a mainframe with a host security module and PCs for key management.

022114 'Communicating with chaos'
S Hayes, C Grebogi, S Ott, *Phys. Review Letters v 70 no 20 (17 May 1993) pp 3031 - 3034*

The authors report using a chaotic oscillator to encode information. This had two attractors in phase space whose values at predetermined times encode '0' and '1' respectively; small control perturbations can be used to drive the output temporarily into the required region. More complex oscillators can be used to hide multiple signals in seemingly random noise.

022115 'Network Security via DNSIX'
HA Heller, *Proc NCSC 92 pp 429 - 437*

Harris has built a prototype compartmented mode workstation which supports the DNSIX protocol of the US Department of Defense Intelligence Information System, and could be made available as a commercial product. Its functionality (and the DNSIX protocol) are described.

022116 'Up-to-date CHAPS'
D Jones, *Banking World (Dec 92) p 43*

The UK clearing system CHAPS should be upgraded by mid-1995 from end-of-day settlement to real time operation. This will work by updating balances held at the Bank of England, and will reduce the system's exposure in the event that a member fails.

022117 'Walking the tightrope at Swift'
D Jones, *Banking World (Dec 92) p 43*

This article surveys international file transfer services for the banking sector. The two main players are Swift and TIPA-NET, and there are a number of proprietary systems such as Tempo and TAPS.

022118 'Home banking by smart phone'
D Jones, *Banking World (Feb 93) p 36*

UK banks are considering the introduction of a low cost terminal developed by Bell labs, which is essentially a phone with an LCD touch screen. This should overcome a number of the shortcomings of current telephone banking systems.

022119 'Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks'
LT Heberlein, B Mukherjee, KN Levitt, *Proc NCSC 92 pp 262 - 271*

The authors report an extension of their previous intrusion detection system to wide area networks such as the Internet. Although reporting to local security managers, it will accumulate information from a range of nodes; experience of penetration attacks shows that this is necessary. The audit implications of remote login are discussed; they might be tackled with such a system.

022120 'AS/400 software security'
K Lester, *Computer Audit Update (Jan 93) pp 2 - 6*

This article describes the security features built into the hardware and software of the IBM AS/400 and how to activate them. It covers hardware keylock, changing the default passwords of powerful users, setting up user profiles, restricting file access and setting password system parameters.

022121 'The Alexandrine Codex: no longer completely an enigma'
G Maro, *SPRC 93 pp 70 - 79*

The author reports the cryptanalysis of the Alexandrine codex, which is the earliest document containing a (primitive) decimal system. As a result, it is ascribed to Fibonacci and dated 1222.

022122 'New dimensions in data security'
KH Mundt, *Proc NCSC 92 pp 438 - 467*

A 160Mbit/sec DES chip is described, which has the features that its S-boxes can be soft loaded, and that key set-up is fast. It is available as a chip, or in an ISA or microchannel bus card with supporting software to provide PC file security.

022123 'Defense against computer AIDS'

HB Peele, *Proc NCSC 92 pp 101 - 119*

This article describes the functionality of the US Air Force PC security toolbox. In addition to controlling viruses, copyright violations and unauthorised shareware, it looks for classification violations, including those which can arise from appended data and from residue data in unallocated memory such as DOS buffers.

022124 'Quantum cryptography and secure optical communications'

SJ Phoenix, PD Townsend, *BT Technology Journal v 11 no 2 (April 1993) pp 65 - 75*

The authors provide an overview of quantum cryptography and describe the state of the engineering art. The idea is to construct a channel on which eavesdropping is impossible due to Heisenberg's uncertainty principle. Previous implementations based on Pockel's cells had been limited to a few bits per second; but optical parametric amplifiers and silicon avalanche photodiodes give the prospect of data rates as high as 1 Mbit/sec and ranges of up to 50Km.

022125 'A physical layer security system for IEEE 802.3/(ISO 8802/3) protocol based local area networks'

FSF Poon, MS Iqbal, *Bilkent proceedings v 1 pp 148 - 154*

The authors describe a CSMA/CD scheme which uses a stream cipher to provide transmission security at the physical layer of the network. The mechanism encrypts CSMA/CD data frames and does not require any changes in the existing hardware and software of the network.

022126 'A New Approach to Cryptographic Facility Design'

J Press, *ICL Technical Journal v 8 no 3 (May 93) p 492 - 505*

This paper describes the Cryptgraphic Support Facility (CSF) available with ICL products, and the key management service which it implements. It has an object-oriented design philosophy which allows easy algorithm replacement; thus applications such as access control in distributed systems can be implemented independently of algorithm details, which mitigates the effect of national security and export restrictions. The mechanisms used specify one of a number of primitives (secret key algorithm, public key algorithm, random number generator, key generator) and a security level (low, medium or high).

022127 'Smart cards get the hard sell'

M Rowe, *Banking technology (Mar 93) pp 34 - 36*

The French banks' decision to phase out magnetic strip cards in favour of smartcards has been attacked vigorously by retailers; as many as 200,000 of them may have to purchase electronic terminal systems at perhaps Ffr15,000 each. This decision was justified on security grounds. American Express also attacked it as undermining confidence in their card.

022128 'Criticism of ISO CD 11166 Banking: Key Management by Means of Asymmetric Algorithms'

RA Rueppel, *SPRC 93 pp 191 - 198*

The author shows that the ISO draft standard CD 11166, which was developed largely for SWIFT, fails to meet the basic ISO requirement for standards. In particular, it is ad hoc, proprietary and has an unsound architecture; the key management layers are interdependent and the combination of encryption and signature used is technically flawed (in that if the encrypted message is larger than the signature modulus, which it is frequently, one has to discard the protocol run and start again).

022129 'New Architecture of Fast Multiplier'
BP Singh, BS Roy, *J. IETE v 39 no 1 (Jan/Feb 1993) pp 349 - 355*

The authors propose a design for a multiplication chip which uses some 20% less gates than previous designs. It involves n^2 AND gates feeding through a Dhurkadas reduction stage to $2n$-1 carry lookahead adders. An illustration is given of its implementation for $n = 16$.

022130 'Designing access control based on need to know requirements in a knowledge base management system'
G Steinke, *Bilkent proceedings v 1 pp 155–161*

In an information system, users should only be permitted to access those objects in the system which they need to know, based on their tasks, assignments and roles. Group Security model is a knowledge base management system developed at University of Passau, which provides assistance in providing such "need to know" based access control.

022131 'A TCB subset for integrity and role-based access control'
DF Sterne, *Proc NCSC 92 pp 680 - 696*

The Extended Access Control Subsystem (ECS) supports a superset of the access control policies mandated by TCSEC; the additions include Clark-Wilson transformation procedures, role-based policies and separation of duties. All of these are implemented using bound operators on list-based data structures.

022132 'The cost of inflexible friends'
The Banker (Jan 1993) p 62

Card fraud in Europe reached $500m in 1991, and its pattern varies roughly with card use: credit cards are more widespread in the US and UK, while cash cards are commoner in Europe.

022133 'Security Protocol Verifier'
E van Wickeren, *Cambridge Workshop*

This article describes a toolkit developed to assist in formal security verifications under ITSEC. Its core algorithm is that whenever a message is sent, you check that the supposed sender could indeed have generated it, and then update a list of all players who could 'receive' it.

022134 'Ingres gives users sense of security'
J Vowler, *Computer Weekly April 22 1993 p 4*

This article reports the launch of the database system Ingres/Enhanced Security, which has an EC E3 security rating, and compares it with Online/Secure from Informix, which is rated B1 in the USA. The performance overhead for the secure Ingres product is claimed to be only 2-3%.

022135 'Auditing Adabas'
A Webb, *Computer Audit Update (Feb 93) pp 9 - 15*

This article gives an extensive and fairly detailed guide to optimising security in the Natural/Adabas database environment. The security system is described, as is its interaction with MVS security features. The key audit points are listed and explained.

022136 'Intrusion and Anomaly Detection: ISOA Update'
JR Winkler, JC Landry, *Proc NCSC 92 pp 272 - 281*

This article describes the Information Security Officer's Assistant, an intrusion detection system based on applying an anomaly model to audit data. It follows the thread of each session and measures certain patterns of behaviour.

2 Operating System and Database Security

022201 'Mediation and Separation in contemporary information technology systems'
MD Abrams, JE Heaney, MV Joyce, *Proc NCSC 92 pp 359 - 368*

The authors examine recent trends in security standards and suggest that separation mechanisms have so far been neglected in both the TCSEC and ITSEC programmes. These standards thus have an overly narrow view of security mechanisms, and have difficulty in coping with multiple access control policies.

022202 'An integrated data protection scheme in a distributed computing environment'
AH Al-Hamed, M Bozyiğit, MI Al-Suwaiyel, *Bilkent proceedings v 1 pp pp 169–175*

The authors describe an integrated security system for message and file protection in a distributed computing system, especially in a local area network. The data security system involves the application of data protection in both the storage and the transmission mediums. These techniques are combined with appropriate key management mechanisms.

022203 'An Access Control Mechanism for Object-Oriented Database Systems'
TA Araki, T Chikaraishi, T Hardjono, T Ohta, N Terashima, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 112–121*

This paper investigates the security problems of object-oriented database systems, and proposes level assignment constraints and an access control mechanism based on the multi-level access control security policy. The proposed mechanism uses a Trusted Computing Base. A feature of the mechanism is that security levels are assigned not only to data items (objects), but also to methods.

022204 'Declarative Foundations of Secure Deductive Databases'
P Bonatti, S Kraus, VS Subramanian *Proc ICDT 92 - Springer LNCS 646, pp 391 - 406*

The authors develop a logic for secure deductive databases. These protect certain explicit secrets, which are defined as formulae in propositional logic, plus a dynamically changing body of implicit secrets, which must also be protected to prevent inference. It is shown that, on certain assumptions, the database will have to lie from time to time in order to protect these secrets. Logics of secrecy and interaction are developed, and model-theoretic semantics for these are described.

022205 'Mandatory policy issues of high assurance composite systems'
J Fellows, *Proc NCSC 92 pp 350 - 358*

The author argues that the lack of A1/B3 distributed systems is not due to a lack of knowhow, but to market forces and a lack of interface standards. The main missing link is a secure remote procedure call supporting mandatory security policies. This would have various implications for security label structures, the location of object management, and multiple access control policies.

022206 'Current endorsed tolls list (ETL) examples - research lessons learned'
C Garvey, A Goldstein, E Anderson, *Proc NCSC 92 pp 93 - 100*

This article describes a publicly worked example of a product (a kernel file manager) evaluated to A1 under TCSEC. This was done using the Gypsy Verification Environment by a novice verifier who was trained on the job. The most important practical lesson was the need to design the system so as to minimise the number of security verification conditions generated; these determine the verification workload.

022207 'Issues in the specification of secure composite systems'
J Hemenway, D Gambel, *Proc NCSC 92 pp 282 - 291*

Today's critical missing technology is the ability to create a secure composite system using a heterogeneous collection of components (some of which may have been evaluated secure). Tow example systems are discussed; the experience drawn from them supports the use of formal methods, and highlights issues of replication, partitioning, dependence, granularity, security labelling and policy consistency.

022208 'SDNS security management'
WA Jansen, *Proc NCSC 1992 pp 574 - 583*

The history and architecture of SDNS are described; it basically consists of an application layer key management system, and lower layer protocols to handle encryption and authentication. The relationship between the various security objects is described; the whole design adheres as much as possible to OSI.

022209 'Integrity and assurance of service protection in a large, multipurpose critical system'
HL Johnson, C Arvin, E Jenkinson, R Pierce, *Proc NCSC 92 pp 252 - 261*

This paper discusses the relationship between criticality and security in the context of USAF systems, where the main aim is often to prevent a denial of service. There is a certain duality in that critical systems need a write-down read-up policy, while secure systems are write-up read-down. Many security concepts go over, and the USAF's criticality classes and authorisation lattice are described. Merging security and criticality does not in general allow any tradeoffs; both must be separately satisfied. Nonetheless there are some common features in practice.

022210 'Composable Trusted Systems'
ES Lee, PIP Boulton, BW Thomson, RE Soper, *University of Toronto report CSRI-272*

This report starts with an explanation and analysis of the American TCSEC/TPSEC and the European ITSEC criteria, and compares the levels of trustworthiness achieved: ITSEC is less detailed, but broader in its scope and more flexible. It proceeds to highlight the difference between guarantee (defined as the design quality of components) and assurance (defined as the quality of the system design and implementation process). This distinction is considered in a number of contexts, such as with security standards (where both TCSEC and ITSEC set out to achieve assurance but tend to deliver only guarantee). It goes on to consider what formal modelling resources are available to a designer who seeks a high level of assurance about a system composed of trusted components, and examines the approaches of McCullough, Johnson & Thayer, Guttman & Nadel, Yu & Gligor, Clark & Wilson, Sutherland and McLean. All of these suffer drawbacks of one kind or another, and finally an alternative is produced. This is called the possibilistic flow model, and a theorem is proved to the effect that this model is composable.

022211 'Some Combinatorial Aspects of Time-Stamp Systems'
R Lori, E Sopena, *European Journal of Combinatorics v 14 no 2 (Mar 93) pp 95 - 102*

Time-stamp systems, as defined by Israëli and Li, are digraphs which express successor relations in distributed computing systems and are similar to Erdős' definition of tournaments. A number of combinatorial results are proven; lexicographical products can be used to build such systems of arbitrary order.

022212 'An access control method for internetwork communications'
FSF Poon, MS Iqbal, *Bilkent proceedings v 1 pp 162–168*

The authors describe an access control method which is based on RSA, and a message authentication method based on DES. These methods are used together to form an access control policy for sharing of resources in interconnected networks of different organizations.

022213 'System Dependability'
B Randell, *Future Tendencies in Computer Science, Control and Applied Mathematics, Springer LNCS 653 pp 21 - 50*

This article presents an overview of EC funded work on predictably dependable computing systems, and in particular the achievement of security and reliability by means of object-oriented fragmented data processing. This is based on the observation that the information which we wish to keep secret may reside in the relationship between data items (eg, the names and salaries in a payroll file). Thus by fragmenting the data in a suitable way, we can process it on an untrusted distributed system.

022214 'Noninterference, Transitivity, and Channel-control Security Policies'
J Rushby, *SRI report CSL-92-02*

Channel control security policies specify how information may flow between domains. They thus generalise the upwards-only flow of Bell-LaPadula and other multilevel systems; they provide extra descriptive power in that they can, for example, deal with systems which have a downgrading mechanism. In such a system, an unclassified user may see top secret data if and only if it passes through the downgrader, and so to model such a system using the noninterference ideas of Haigh and Young, we must change the model so that the 'interferes' relationship becomes intransitive. This is done, and an unwinding theorem for the intransitive case is presented.

022215 'A lattice interpretation of the Chinese Wall policy'
RS Sandhu, *Proc NCSC 92 p329 - 339p*

Chinese Wall security policies are desirable in many practical systems, but the Brewer-Nash model has the problem that a user who reads from more than one source cannot thereafter write at all. An alternative formalism is presented, which is based on lattices and does not suffer from this problem.

022216 'Implementation considerations for the Types Access Matrix model in a Distributed Environment'
RS Sandhu, GS Suri, *Proc NCSC 92 pp 221 - 235*

The first author's typed access matrix model is simplified to operate on one object at a time, and this restricted version is conjectured to retain most (if not all) of the power of the original model. It is used to implement originator control of documents in a way which is congenial to client-server systems, as no distributed commit is required.

022217 'Potential benefits from implementing the Clark-Wilson integrity model using an object-oriented approach'
CA Schiller, *Proc NCSC 92 pp 482 - 493*

The author discusses how to use Clark-Wilson with object oriented systems. It can be implemented using four major kinds of object (user, authorisation, log, and application), and methods such as 'verify', 'promote', 'transform' and 'record'. The practical security benefits of object orientation include typing and encapsulation.

022218 'Protected groups: an approach to integrity and secrecy in an object oriented database'
JM Slack, EA Unger, *Proc NCSC 92 pp 513 - 522*

The authors define a 'protected group' to be a set of objects which will accept messages only from a set of interface objects, and show how one can implement various access control, inference control and integrity properties by partitioning a database into protected groups.

022219 'Knowledge-based inference control in a multilevel secure database management system'
B Thuraisingham, *Proc NCSC 92 pp 319 - 328*

Inference control tools should be available not just during transaction processing, but also during database design and to advise security officers. Knowledge based systems can be used in this application: an appropriate strategy may be to represent the inference restrictions at high level as conceptual graphs, and then reduce them to rules and frames for execution. A truth maintenance system can then be used to ensure consistency at all levels, even where cover stories are used to deal with polyinstantiation.

3 Security Management and Policy

022301 'Accreditation: is it a security requirement or good management practice?'
TE Anderson, *Proc NCSC 92 pp 1 - 8*

The author clarifies the distinction between certification and accreditation (as these terms are used by the US military): the former refers to documentation and approval of security measures, while the latter is the act of managerial acceptance of the residual risk. Accreditation occurs in any case when is system is run live for the first time; formalising the process ensures that documentation (of contingency plans, configuration, training, etc) exists and will be updated as necessary. It is the final and most important part of the security jigsaw.

022302 'E-Mail Privacy and the Law'
C Axsmith, *Proc NCSC 92 pp 120 - 125*

This article discusses the legal implications of email privacy in the USA. The key test (deriving from the fourth amendment) is whether there is a reasonable expectation of privacy under the circumstances; if there is, then email monitoring might not be admissible as evidence in a criminal prosecution, and monitored employees might sue. For this reason, it may be prudent to inform employees that they may be monitored.

022303 'Managing Complexity in Secure Networks'
D Bailey, *Proc NCSC 92 pp 777 - 783*

Current security models depend on a single person being able to understand all the information flows and controls in a system. This assumption is becoming less and less realistic, and partitioning networks into comprehensible subunits is becoming less and less feasible as products like Sun's NFS hide the network activities from the user. New paradigms are needed to deal with complex systems, and two candidates are the 'secure telephone' and 'VP protection' model. In these, an island of trust is created around a data stream (or object), or around a user.

022304 'Seeking Security'
P Barsook, *Byte v 18 no 6 (May 1993) pp 119 - 128*

Mainframe security systems and expertise do not go across to distributed architectures particularly well. A number of users' and suppliers' views on the problem are presented; issues include encrypting email, distributed security standards, secure unix, and cultural/management problems.

022305 'On the Meaning of Safety and Security'
A Burns, JA McDermid, JE Dobson, *University of Newcastle upon Tyne report no 382 (1992)*

The authors discuss two distinctions between safety and security. In the first, a safe system cannot harm us, while a secure system cannot be used by others to harm us. In the second, the distinction relates to how serious the harm is: a safety critical system could do absolute. or permanent, harm if it failed, while a security critical system could only do relative harm. The two are related in that (at least in commercial organisations) security usually relates to competitive advantage (whose loss is a relative matter) rather than to human life, whose loss falls into the category of absolute harm.

022306 'Priorities for LAN security - a case study of a federal agency's LAN security'
SH Chang, *Proc NCSC 92 pp 503 - 512*

This article describes applying the NIST method of risk assessment and management to a Banyan Vines system in a US government agency. This involved tabulating the level of risk (as threat likelihood times potential damage) for each threat scenario, and deriving a list of security priorities. In this case, the list was headed by poor password choice and lack of physical security.

022307 'Some More Thoughts On The Buzzword 'Security Policy'
DM Chizmadia, *Proc NCSC 92 pp 651 - 660*

The concept of 'security policy' is elusive; it has a number of different definitions, of which those in the Orange Book, ITSEC and Sterne's Oakland 91 article are examined. These definitions operate at the management and technical levels, but it seems that greater granularity than this is required; a more detailed hierarchy would be better able to express the underlying requirements in a way meaningful at each step of the system development process.

022308 'EDI Security in Practice'
CJ Clark, *Computer Fraud and Security Bulletin (Jan 93) pp 9 - 13*

The authenticity and integrity of EDI transactions under ISO 9735 are only protected by plaintext mechanisms such as the sender's name and a unique reference number; integrity and confidentiality are left to the network service provider. New recommendations from the Joint Security Working Group at EDIFACT (a UN body) include the discretionary use of encryption mechanisms; this will expose commercial users to issues of government regulation and key management which they have so far avoided.

022309 'Risk Assessment'
BS Collins, *Computer Fraud and Security Bulletin (Jan 93) pp 13 - 16*

Organisations which adopt EDI could be assuming new risks, and should scrutinise their system's rules closely. Although commercial organisations understand paper security mechanisms (such as recorded delivery and multiple ledger entries), the corresponding information security mechanisms, such as encryption, are unfamiliar, and so EDI may transform business practices in ways which are not tested or even understood.

022310 'Risk management of complex networks'
R Cox, M O'Neill, W Price, *Proc NCSC 92 pp 544 - 553*

Current US Department of Defense guidance is inadequate for complex evolving networks, especially where the system has two or more interconnected networks, two or more responsible organisations, and no overall policy. A methodology for risk management and accreditation of such networks is presented, including checklists for security policy, architecture and accreditation strategy.

022311 'Electronic measurement of software sharing for computer virus epidemiology'
L de La Beaujardiere, *Proc NCSC 92 pp 126 - 133*

The author argues that there is a need for more accurate data on software sharing patterns, and proposes using test viruses to gather this information.

022312 'Authentication Standards'
M De Soete, K Vedder, *SPRC 93 pp 207 - 218*

This article provides a review, with 42 references, of international standards work on authentication protocols. This work includes such fine detail as the directive that the verb 'shall' should be used instead of 'must'; nonetheless, terminology and definitions are still not consistent across the range of issued standards and participating bodies. ISO 9598 is discussed in particular; this is derived from CCITT X.509 and deals with entity authentication. ISO 9797 on message authentication codes is also mentioned.

022313 'Stealth Virus Attacks'
J Dehaven, *Byte v 18 no 6 (May 1993) pp 137 - 144*

This article warns of possible 'cruise' viruses, which would be targetted at specific applications, such as accounting software, and deliver a 'payload' which might, for example, send a cheque to the perpetrator. A list of anti-virus software vendors is included.

022314 'RIPE Integrity Primitives'

B den Boer, JP Boly, A Bosselaers, J Brandt, D Chaum, I Damgård, M Dichtl, W Fumy, M van der Ham, CJA Jansen, P Landrock, B Preneel, G Roelofsen, P de Rooij, J Vandewalle, *EC RACE Document R1040*

This reports an EC project to define integrity primitives. It contains recommendations for DES-based message authentication and manipulation detection codes, a hash function (RIPEMD) derived from MD4, a one-time authenticator, and authentication protocols based on RSA and on hash functions with a secret key. There are also general observations on the implementation and security of RSA.

022315 'A New Paradigm for Trusted Systems'

DE Denning, *Proc NCSC 92 pp 784 - 791*

The author summarises the drawbacks of the Orange Book approach to computer security and argues that a new paradigm is needed. She points out that trust is relative to a domain of action: for example, a person may be trusted to be a good cook without being trusted to be a good pilot. Similar pragmatic considerations show that a system will acquire trust from its users over time if it performs well; in effect, there is a marketplace in which individuals, systems and products acquire trust. Thus in the new paradigm, trust should be an assessment rather than a property.

022316 'Role-based Access Controls'

D Ferraiolo, R Kuhn, *proc NCSC 92 pp 554 - 563*

In many commercial applications, the most appropriate access control method is to assign access privileges to roles (such as teller or accountant) rather than to follow the military practice of basing access control on the sensitivity of information.

022317 'Auditing the contingency plan'

D Firth, *Computer Audit Update (Jan 93) pp 11 - 15*

As contingency plans represent a major investment, they should be audited; and the article discusses how to do this. One key issue is how far the auditor can get involved in testing the plan and monitoring the results; he must in any case check that the tests are realistic, that the plan will be maintained effectively, and that it is focussed on business recovery rather than technical interests.

022318 'Concept paper: an overview of the proposed trust technology assessment program'

EE Flahavin, PR Toth, *Proc NCSC 92 pp 84 - 92*

Under the trust technology assessment program, US security product evaluations at level B1 and below will be delegated from the NSA to accredited laboratories. These will be supervised by a new product Evaluation Management Board to ensure that these evaluations will be fair and credible. The program objectives are to provide compatibility with the EC's ITSEC program, and to increase the number of evaluated products.

022319 'The Search For Client/Server Security'

B Francis, *Datamation v 39 no 9 (May 1993) pp 39 - 43*

Client-server systems are more vulnerable than mainframes for two main reasons - additional threats such as viruses, and a relative lack of good security tools. A number of products are mentioned, and their features are discussed; central signon is a problem. Many developers pay the price by having to retrofit security features to their applications.

022320 'The Second Conference on Computers, Freedom and Privacy'

LJ Hoffman (editor), *published by the ACM (1993)*

This book is an edited transcript of the discussions at the 1992 conference on computers, freedom and privacy. These discussions cover a very wide range of topics, including civil liberties; data protection; the common carrier (or other) status of value added networks; the ethics of using DNA sequencing in law enforcement; private collection of personal information; government regulation of cryptology; public access to government records; and the breadth of access to the information society's resources in general.

022321 'Information system security engineering: cornerstone to the future'
DM Howe, *Proc NCSC 92 pp 244 - 251*

System security engineering is defined as an empirically based methodology for composing and evaluating systems within a structure of standards, and which encompasses operation as well as planning, design, implementation and operation.

022322 'EDI Security'
P Kenny, *Computer Fraud and Security Bulletin (Jan 1993) pp 7 - 9*

This article describes how EDI is interfaced to banking systems, and briefly outlines the UN/EDIFACT message level security recommendations.

022323 'Epidemiology of computer viruses'
JO Kephardt, SR White, DM Chess, *IEEE Spectrum v 30 no 5 (May 93) pp 27 - 29*

The authors present statistics of virus incidents reported to IBM in the two years to May 1993. The infestation rate appears to be 1 per 1000 PCs per quarter, which is much lower than many authors had claimed; less than 15% of the 1,500 known viruses were observed (and most of these were only reported once). The applicability of medical epidemic models is discussed; these are limited by the different topology of software intercourse (sharing of software is highly localised) and so predict higher infection rates than are actually observed. Nonetheless two medical results go over: firstly, there is an epidemic threshold, ie a self-sustaining level of infection; and secondly, the most effective organisational countermeasure is centralised reporting and response using selective vaccination.

022324 'Use of a CASE tool to define the specifications of a trusted guard'
R Lazar, JH Gray, *Proc NCSC 92 pp 728 - 737*

This article describes the application of a Yourdon variant to product documentation for verifying and maintaining a NASA communications processor which handles satellite data relay for both classified and unclassified users.

022325 'Smart moves gain ground'
R Martin, *Cards International no 81 (Mar 4, 1993) pp 8 - 9*

This article reports the discussions at the Smart Card 93 conference. Smartcards have at last been accepted by VISA for offline PIN checking; and views expressed by VISA, Barclays and Lufthansa are reported.

022326 'Fraud: the Asian defences'
E McCullough, *Cards International no 82 (Mar 19, 1993) pp 9 - 10*

Hongkong and Shanghai bank found its safeguards being overwhelmed by card counterfeiters in 1991, as local criminals learned to cope with both magnetic strips and holograms. Their reaction was a rapid move to online terminals, which 85% of local merchants now have. The problem now is counterfeiting of overseas cards; overseas banks should stop this by implementing card verification values and abolishing floor limits.

022327 'Keeping faith with Electron'
E McCullough, *Cards International no 81 (Mar 4, 1993) pp 10 - 15*

This article reports an interview with VISA chief executive Chuck Russell in which he describes VISA's fraud experience and strategy. The cost was $700m last year, of which four-fifths was due to theft (including mail intercepts) and one-fifth due to counterfeiting. This level does not justify a move to smartcards. Instead, the strategy is to introduce many more online terminals, to adopt card verification values worldwide, and introduce a tamper-resistant magnetic strip (for which the standards will be announced in the fourth quarter of 1993). Once these elements are in place, PINs will be introduced at the point of sale; work on signature recognition has been abandoned.

022328 'Security within the DODIIS reference model'
BW McKenney, *Proc NCSC 92 pp 620 - 630*
This article describes the US Department of Defense Intelligence Information System, and in particular the reference model used for planning procurement and upgrade, which is based on NIST's Application Portability Profile (APP). This model interacts with open and government standards in a number of ways, and provides a number of security services to applications.

022329 R Morris, *Cambridge Workshop*
In this talk, the speaker (who is chief scientist at the US National Computer Security Center) describes the NSA's mission and its approach to designing secure systems. The main advantage that the agency has over civilian experts is wide experience of how cryptographic systems fail, and the thoroughness with which threats are examined. It is always assumed, for example, that there will be disloyal systems staff, and this treachery is considered to be a mandatory component of all system designs. The main management problem is accepting and managing the residual risks which are left after all the economic technical security measures have been taken.

022330 R Morris, *Cambridge Workshop*
Civilian computer security systems could be most improved by better threat analysis; information must be valued by means of a realistic appraisal of who will spend how much money to attack it. One should not ask 'if I use this system, can a bad guy read my traffic?' as the answer is always yes (if he spends enough money). The right question is 'Is this system a prudent custody of the information for which I am responsible?' More attention should also be paid to generating good message keys, using algorithms in appropriate modes, and clarifying concepts such as 'trust'.

022331 Toward a model of security for a network of computers'
WH Murray, P Farrell, *Proc NCSC 92 pp 707 - 716*
The authors address the problem of what statements may be made about the security of populations of computers. They model the cost of attacks and the value of a successful attack.

022332 'An approach to multilevel security (MLS) acquisition'
W Neugent, *Proc NCSC 92 pp 18 - 27*
This article provides interim guidance for US government organisations acquiring multilevel systems, pending a firm Dod policy on the subject. It provides a road map to the process of selecting the needed capabilities, developing a concept of operations, getting approval, designing the security architecture, acquiring and integrating products, and obtaining certification and accreditation.

022333 'General issues to be resolved in achieving multilevel security'
W Neugent, *Proc NCSC 92 pp 213 - 220*
This article describes the US government's multilevel security program, the various management issues and compromises involved in operating without suitable products, and the strategies being adopted by the US defense community. These interim strategies carry a risk that accreditation of many dubious systems could create a body of precedent which would undermine policy.

022334 'Companion document series to the trusted database management system interpretation'
LA Notargiacomo, V Ashby, V Doshi, J Filsinger, S Jajodia, R Ross, *Proc NCSC 92 pp 57 - 65*
This paper gives an overview of a number of documents developed by Mitre for the US National Computer Security Center. These provide interim guidance in the field of trusted databases, which is felt to be too fast moving for a firm policy, but complex enough to require some guidance. The documents cover interference problems, aggregation problems, entity and referential integrity, auditing, polyinstantiation and discretionary access control.

022335 'Security Management: Using the Quality Approach'
RW Owen, *Proc NCSC 92 pp 584 - 592*

This article describes the security and quality management techniques introduced at NASA's Mission Operations Directorate when it was downgraded from a classified site to an unclassified but sensitive one. This actually involved tightening security, especially against 'commercial' security threats such as viruses and hackers.

022336 'A model of risk management in the development life cycle'
CR Pierce, *NCSC 92 pp 389 - 398*

As systems become more disparate and dispersed, the US Department of Defense is having to extend the traditional scope of computer risk management from the traditional approach of taking and examining a snapshot of a system to consider its whole life cycle. Standards based on this are currently being developed for the USAF. This allows one to cope with existing systems which need reassessment and upgrade, and with the problem that security levels and requirements are significantly changed during the development process.

022337 'Standard certification - progression'
CR Pierce, *Proc NCSC 92 pp 670 - 679*

This paper reports the activities of an interservices group in the US military which works on standardising the certification, risk management, evaluation and accreditation of secure systems, together with training and education requirements for development and operations staff. Its goal is to maximise the sharing of information, tools and other resources.

022338 B Preneel, *Cambridge Workshop*

This talk gives an overview of current international standards activity in the authentication field. The structure of the various international bodies, committees and working groups is described, as is the state of play of proposed standards for protocols using symmetric and asymmetric algorithms, irreversible functions and zero knowledge.

022339 'Interception and modification of communication channels'
B Robertson, D Pullen, *Computer Audit Update (Feb 93) pp 3 - 8*

This provides an overview for managers and auditors on communications security threats including tapping, configuration change, jamming, flooding, and various active attacks on protocols and messages.

022340 'Hardware/software security testing'
B Robertson, D Pullen, *Computer Audit Update (Jan 93) pp 7 - 11*

The authors propose a regime for system security testing which involves risk analysis and structured testing. For a security module, this would include testing that the encryption algorithm is correctly implemented, that keys are generated at random, that the units are actually tamper resistant and that unit failures are properly reported. Software testing is also discussed.

022341 'Re-use of evaluation results'
JD Smith, *Proc NCSC 92 pp 534 - 543*

This article considers how ITSEC results can be re-used, and describes the relevant sections on effectiveness and correctness. The assumption that systems and products can be considered in the same way is not in general true, and composition effectiveness must be analysed for suitability, binding, construction vulnerability and ease of use.

022342 'Backup systems: what to look for'
A Solomon, *Computer Fraud and Security Bulletin (Feb 93) pp 15 - 18*

The author discusses the advantages and disadvantages of diskette and tape backup, and gives a number of hints on how to use these effectively.

022343 'Computer forensics: an introduction'
P Sommer, *Computer Fraud and Security Bulletin (Feb 93) pp 10 - 15*

This article discusses the techniques which can be used to obtain and secure computer evidence, and describes the relevant parts of the UK's civil and criminal evidence law. The former is actually stricter on the admissibility of computer records; this is of concern as many computer misdeeds involve insiders and thus become matters of contract and employment law.

022344 'A Model for the Measurement of Computer Security Posture'
L Sutterfield, T Schell, G White, K Doster, D Cuiskelly, *Proc NCSC 92 pp 379 - 388*

The USAF is trying to improve its security posture by statistical process control methods adopted from the Japanese practice of 'total quality management'. A taxonomy of concerns is presented; this covers various layers of management activity, from the overall system mission down through policies, procedures, training and controls to technical assurance measures.

022345 'Computer crime: investigating inside the corporation'
H Topton, *Computer Fraud and Security Bulletin (Feb 93) pp 4 - 10*

Investigations of computer crime are only 10% technical; the other 90% consists of standard police work, which is summarised in this article. It surveys issues of evidence, interrogation techniques, and presentation of an investigation report.

022346 'A Security Reference Model for a Distributed System and Its Applications'
V Varadharajan, *Proc NCSC 92 pp 593 - 619*

Various threats against distributed object oriented systems are described, together with the technical and management functions needed to counter them. Solutions may be based on embedding a security module in each client and server; this is illustrated with reference to building an office system out of portable PCs.

022347 'Should Encryption be Regulated?'
P Wayner, *Byte v 18 no 6 (May 1993) pp 129 - 134*

This article considers the conflict between the government's and the citizens' interests in regulating cryptology. The options discussed include no regulation, weak encryption, and Micali's 'fair cryptosystems'.

022348 'Computer security and total quality management'
GB White, L Sutterfield, C Arvin, *Proc NCSC 92 pp 66 - 75*

This article discusses how the US federal government's 'total quality management' program interacts with security. The program and its underlying theory are described; security failures are seen as largely due to the lack of a defined institutional security process which can be subjected to the continual incremental improvement on which this program is based. A checklist on applying quality management to security is provided.

022349 'Contingency planning: issues and challenges'
K Wong, *Computer Fraud and Security Bulletin (Mar 93) pp 11 - 19*

The 1992 IRA bomb in London taught that paper, as well as magnetic media, need backing up offsite; a clear desk policy (under which all paper is locked up at night) is also highly advisable. Further problems are posed by client/server architectures, mixed vendor sites, facilities management contracts, and value added networks such as EFT and EDI.

4 Formal Methods and Protocols

022401 'Uses of Formal Methods'
RJ Anderson, *Cambridge Workshop*

Formal methods have been extensively used to verify hardware, system software and specifications, but much less so to check application software (where most of the mistakes occur). One approach was that taken in work on a smartcard payment system, where the security depends on a trusted application kernel which is implemented in smartcards. A further problem is that formal attempts to specify the properties of cryptographic algorithms have run into trouble; the concept of collision freedom is particularly problematic.

022402 'Why Cryptosystems Really Fail'
RJ Anderson, *Cambridge Workshop*

Initial results of a survey into the failure modes of electronic banking systems are described. Although most cryptosystem designers focus on highly technical attacks, the frauds which actually occurred were all due to implementation errors and poor management. This raises questions about the role of formal methods and the possibility of introducing new paradigms, such as from the aviation industry and from other branches of engineering concerned with safety critical systems.

022403 'Methods to Securely Realize Caller-Authenticated and Callee-Specified Telephone Calls'
T Asano, T Matsumoto, H Imai, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 88–95*

This paper presents two methods for securely realizing caller-authenticated and callee-specified calls over telecommunication networks with terminals that accept IC cards having Key Predistribution System based cryptographic functions. In the proposed protocols, a caller and a callee authenticate their partner by verifying that the partner is the proper owner of a certain IC before starting their conversation. Unlike ordinary services with caller-ID indication, the privacy of the caller and the callee is protected even if they do not prepay their telephone charges.

022404 'Methods for Reasoning about Cryptographic Protocols'
P Bieber, *Cambridge Workshop*

Protocol verification logics fall into three categories. The first is complexity-based and focusses on algorithms; the second is word-oriented and exemplified by the work of Dolev-Yao, Meadows, etc; while the third is belief-oriented and includes BAN. Work at CAP/CERT has been directed towards constructing an abstract layer which builds a bridge between definitions of properties (such as authentication) and concrete descriptions of protocols. It allows flexibility in defining properties, such as a gradation between the 'obligatory' and 'authorised' sender of a message.

022405 'Security Architectures using Formal Methods'
C Boyd, *Cambridge Workshop*

This talk emphasises the formal symmetry between confidentiality and authentication; the former means that you need the key to read the data, while the latter means that you need the key to write it.

022406 'Document Integrity in CSCW'
B Christianson, *Cambridge Workshop*

A project is described which provides authentication services in an open environment using only a trusted name server. This server maintains a list of authorised documents (and their hash values) and enforces whatever upgrade policy has been agreed. The idea is to minimise the amount of code which everybody has to trust. The prototype provides control over development of a document (such as program source code), but can be generalised to provide a unified approach to access control, integrity, audit and concurrency conflict resolution in object oriented systems.

022407 'PM: a Unified Automated Deduction Tool for Verification'
G Fink, L Yang, M Archer, *Proc NCSC 92 pp 473 - 481*

The authors describe Proof Manager (PM), a gnuemacs-based front end for a number of theorem provers (including HOL and Boyer-Moore). This can be used for both hardware and software verification; it allows a more direct and visual control of the proof process, and the ability to provide proof summaries.

022408 'On the Design of Authentication Mechanisms'
W Fumy, *SPRC 93 pp 199 - 206*

The author describes an approach to secret key authentication, and provides three sample authentication protocols.

022409 'Inter Realm Authentication'
V Gligor, *Cambridge Workshop*

Three ideas are introduced: firstly, in order to build systems where there is no hierarchy of authentication servers, one needs a formalism of introduction, which is introduced (its primitive is 'a accepts b's word about c'); secondly, a 'splicing and decomposition invariant' is proposed which enables the effect of known plaintext/ciphertext pairs to be checked; and thirdly, there is a need for an effectiveness analysis which ties up a protocol's security properties with actual threats (otherwise protocols may be seriously overengineered).

022410 'Thoughts on Cryptographic Protocols'
L Gong, *Cambridge Workshop*

Most formal methods proposed to date have problems with at least one valid protocols. The heart of the matter appears to be freshness; this breaks the symmetry between confidentiality and authentication. It is not equal to randomness (as counters can be used as nonces), and also not equal to replay (as one must also guard against interleaving attacks). One solution may be to restrict usage in such protocols, just as structured programming methods discourage the use of 'goto' statements; errors occur when people try to be smart.

022411 'Some Metrics of authentication protocols'
L Gong, *Cambridge Workshop*

A table is presented of proven results on the number of messages required in different types of protocol (such as whether one or both parties choose the key, or whether the server does).

022412 'ProofPower Implementation of BAN Logic'
D King, *Cambridge Workshop*

This talk describes an ICL product, called 'ProofPower', which verifies cryptographic protocols by implementing BAN using an extension of HOL. The semantics of the system are discussed. It is capable of generating the results of the original BAN paper.

022413 'Formal Methods and testing secure Open Systems'
R Lampard, *Cambridge Workshop*

This gives an overview of formal methods research at the UK National Physical Laboratory. Its goal is to develop new techniques for testing equipment for ITSEC, which must include tracing the evaluation all the way back to the relevant standards documents.

022414 'Confidentiality and Authentication'
WB Mao, C Boyd, *Cambridge Workshop*

A version of Otway-Rees which was recently proposed in the literature, and which can be verified as correct using BAN, is shown to have a flaw: if it is implemented using DES with Cipher Block Chaining, and the block boundaries coincide with the boundaries between the protocol elements, then a splicing attack is possible.

022415 ‘A logical language for specifying cryptographic protocol requirements’
C Meadows, *Cambridge Workshop*

The Navy Research Labs protocol analyser models cryptographic protocols using words and reduction rules. Its strategy is to track words known by the intruder, together with local state variables and transitions; to find ways to trim the state space, and then exhaustively search for potential security violations.

022416 M Purser, *Cambridge Workshop*

This talk describes a secure email pilot project which is being used to explore the organisational and other practical issues of such services. The identified problems include the security of the workstation/LAN interface, security software integrity, audit control, replacement of master keys and the fact that key certificates must be preserved indefinitely in order to resolve future disputes.

022417 ‘Disaster recovery Planning’
M Roe, *Cambridge Workshop*

This talk considers the problem of how an organisation can recover from a security disaster (such as a security officer defecting, an algorithm being broken, or a key distribution centre being subverted). It turns out that different protocols have different recovery properties; public key systems are generally more resilient, whereas systems based on symmetric algorithms and a key server (such as Kerberos) are vulnerable to theft or judicial compulsion of the server. Online servers, on the other hand, allow user privileges to be changed more quickly in the event of a defection. The SDNS system, whose servers provide daily changes of public keys for users, gives the best of both worlds.

022418 P Ryan, *Cambridge Workshop*

This talk describes the approach of the UK Defence Research Agency, which is beginning to get interested in sponsoring research in formal methods. Its preference is for CSP and other Oxford formal tools.

022419 ‘Security clauses in the writing and analysis of standards’
B Szczygiel, A Harry, *NPL report 216/93*

Formal methods are not yet expressive enough, in that they fail to capture many security properties which standards documents and testing regimes justifiably require. These include time dependence, error handling, and the relationship of individual security features with each other and with the environment (and especially the operational and other human aspects of the environment). Thus further security clauses are necessary; and these differ from conformance clauses in a number of ways, which are illustrated in the context of covert channels. Security clause characteristics are discussed with reference to the message authenticator algorithm.

022420 ‘Specifying Cryptographic Protocols’
E Snekkenes, *Cambridge Workshop*

A formal logic is presented to deal with impersonation. It uses denotational semantics, and so was easy to implement; but cannot analyse very deeply due to the combinatorial explosion.

022421 ‘Adding Time to a Logic of Authentication’
P Syverson, *Cambridge Workshop*

A recently published protocol of Neumann and Stubblebine is broken by making one of the participants use a public nonce as a session key. This is called a ‘causal consistency attack’, in that it works if the principals fail to notice that their records are inconsistent. The proposed solution is to extend BAN by adding time; this enables the concept of records to be formalised and blocks which have already been seen to be recognised and rejected.

022422 **'A System for Deciding the Security of Cryptographic Protocols'**
H Watanabe, T Fujiwara, T Kasami, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 96–103*

This paper proposes an algorithm to decide the security of cryptographic protocols under several conditions. The approach assumes that a protocol is secure if active saboteurs cannot achieve their goal even though they get any information which is not protected in the system.

022423 R Yahalom, *Cambridge Workshop*

This talk addresses the problem of how to cope with multiple authentication servers, not all of which may be trustworthy. One may trust such servers to identify their neighbours, but not to generate a good session key. It proves that two-way authentication along a chain of n authentication servers needs exactly $n+4$ messages. In other words, with one server, one needs 5 messages, rather than the 6 of Otway-Rees and Needham-Schroder; and with two servers, one needs 6 instead of Kerberos' 8.

5 Secret Key Algorithms

022501 'Designing s-boxes for ciphers resistant to differential cryptanalysis'
CM Adams, SE Tavares, *SPRC 93 pp 181 - 190*

The authors elaborate on the weakness of bent-function-based s-boxes which were pointed out by Biham, and define a new class of boxes whose columns are based on bent functions but whose rows satisfy a number of other criteria. They propose a block cipher algorithm based on these, which has eight rounds and 64-bit key and data blocks.

022502 'Sulla decimazione di sequenze pseudocausali'
M Bucci, A Di Porto, R Menicocci, E Montolivo, *SPRC 93 pp 134 - 142*

Arbitrary terms of a linear congruential sequence can be calculated directly by recursively finding the generators of the 2^k-th decimations and using these as a basis. Similar techniques are described for shift register systems.

022503 'The Data Encryption Standard (DES) and its Strength Against Attacks'
D Coppersmith, *IBM report RC 18613 (81421)*

This report at last reveals some of the design principles behind the DES algorithm, and in particular its S-boxes. These are presented as requirements that a certain number of output bits will change with various patterns of input change; they were designed to ensure rapid diffusion and confusion of bits, and to make the algorithm resistant to differential cryptanalysis. The report also shows that DES generates a large subgroup of $S_{2^{64}}$.

022504 'Block Ciphers Based on Modular Arithmetic'
J Daemen, R Govaerts, J Vandewalle, *SPRC 93 pp 80 - 89*

The authors criticise IDEA for achieving poor diffusion when the key is sparse, and identify more 2^{51} weak keys. They propose instead a new algorithm, called MMB (for 'Modular Multiplication based Block cipher), which has 6 rounds, 128-bit key and data blocks, and a simpler internal structure.

022505 'Cryptanalysis of MUX-LFSR Based Scramblers'
J Daemen, R Govaerts, J Vandewalle, *SPRC 93 pp 55 - 61*

The authors present a recursive algorithm for reconstructing the initial state of a multiplexed feedback shift register system, as used in the European Broadcasting Union MAC/packet family scrambling proposal.

022506 'Statistical independence of a new class of inversive congruential pseudorandom numbers'
J Eichenauer-Herrmann, *Math. Comp v 60 no 201 pp 375 - 384*

The pseudorandom numbers generated by the linear congruential method have undesirable regularities in certain applications. This has led to the development of various nonlinear congruential methods, such as the inversive congruential generators based on taking successive multiplicative inverses with respect to a prime modulus. The author introduces a new class of these generators and analyzes the statistical independence properties of the resulting sequences.

022507 'On Inversive Congruential Generators for Pseudorandom Numbers'
M Flahive, H Niederreiter, *Las Vegas proceedings p 75 - 80*

The authors characterise those inversive congruential generators which have maximal period, and define the maximal dimension of a sequence as the highest dimension of Marsaglia's lattice test which it passes. They then show that the maximal dimension of a maximal period inversive sequence is odd.

022508 'Performance testing of Galois linear group sequences'
G Gong, A di Parto, W Wolfowicz, *SPRC 93 pp 90 - 105*

The authors construct pseudorandom sequences using matrices over finite fields; these are shown to have the same properties as more conventionally generated m-sequences.

022509 'A New Family of Nonbinary Sequences with Large Linear Span'
CK Kim, JJ Komo, *Las Vegas proceedings p 123 - 130*

The authors define a family of sequences with large linear span and low out-of-phase correlation, by generalising the work of No and Kumar on sums of shift register sequences from characteristic 2 to characteristic p.

022510 'How to Strengthen DES-like Cryptosystems against Differential Cryptanalysis'
K Koyama, R Terada, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 63–69*

The authors propose a randomized version of DES in which a key-dependent swapping is used to strengthen DES and DES-like cryptosystems against differential cryptanalysis. This scheme, called RDES, decreases the probability of success in differential attack by decreasing the characteristic probability; for n-round RDES, this is 2^{1-n} times that for n-round DES. As for differential cryptanalysis based on characteristics, 16-round RDES is as strong as 20-rounds DES. The encryption/decryption speed of RDES is almost the same as that of DES with the same number of rounds.

022511 'Nets obtained from rational functions over finite fields'
G Larcher, *Acta Arithmetica v 63 no 1 (1993) p 1 - 13*

The author presents an improvement of a bound of Niederreiter on the discrepancy of a point set obtained from rational functions over a finite field, where the defining function is a monomial.

022512 'Cascade Ciphers: The Importance of Being First'
UM Maurer, JL Massey, *Journal of Cryptology v 6 no 1 pp 55 - 61*

A cascade cipher is at least as hard to break as its first round; it will be as strong as its hardest component if these components commute (as, for example, with additive stream ciphers). A counterexample is produced to illustrate that if they do not commute, then a cascade will in general only be as hard as its strongest component if no use can be made by the opponent of the plaintext statistics.

022513 'The kinetic protection device'
G Mayhew, R Frazee, M Bianco, *Proc NCSC 92 pp 310 - 318*

The authors describe a stream cipher which is to be incorporated in export versions of a tactical radio and navigation systems manufactured by Hughes. Its keystream is a nonlinear function of 6 bits drawn from a 61 bit feedback shift register. The base key is the feedback polynomial and the choice of nonlinear function, while the message key is the initial state. The device's design considerations and test regime are described.

022514 'Cryptanalysis of a two-stage Gollmann cascade generator'
R Menicocci, *SPRC 93 pp 62 - 69*

The author presents an attack on a two-stage clock controlled shift register. This is based on finding a sufficiently long string of 1's or 0's in the output keystream and inferring from this that the driving register is outputting zeros toward the end of this string.

022515 'Computer data ciphering by use of Chinese remainder theorem'
M Mirković, B Pavić, M Vujasinović, R Bojović, *Bilkent proceedings v 1 pp 183–187*

The authors suggest using the Chinese remainder theorem for secret-key data encryption: the keys are relatively prime moduli, and the residues are the data records to be encrypted.

022516 ‘Finite Fields, Pseudorandom Numbers and Quasirandom Points’
H Niederreiter, *Las Vegas proceedings p 375 - 394*

This article discusses applications of pseudorandom sequences to problems in numerical analysis, and the generation of such sequences by the multistep method, inversive congruential generators and general feedback shift registers.

022517 ‘Recent Advances in the Theory of Finite Fields’
H Niederreiter, *Las Vegas proceedings p 153 - 163*

This is a survey article, with 70 references, on computational aspects of finite field theory. It focusses on polynomial factorisation and the construction of irreducible and primitive polynomials, field isomorphisms and normal bases.

022518 ‘Period of sequences of primitive polynomials’
B Park, H Choi, T Chang, K Kang, *Electronics Letters (Feb 1993)*

If f is primitive over $GF(q)$ of degree n with root α, and $\gcd(k, q^n)$=1, then let f^j be the minimal polynomial of α^{kj}. It is shown that the number of distinct elements of $\{f^j\}$ is equal to the q^n-order of k, and an algorithm is given for calculating this.

022519 ‘On Nonexistence of Generalised Bent Functions’
DY Pei, *Las Vegas proceedings p 165 - 172*

The author shows that there are no generalised bent functions over Z_p^n where n is odd and q = $2p^r$ for $p \equiv 3$ or 5 (mod 8) or where $n = 1$ and $q = 14$.

022520 ‘Bent Permutations’
J Pieprzyk, *Las Vegas proceedings p 173 - 181*

The author defines a permutation in $GF(2^n)$ to be bent if it achieves the same nonlinearity as a bent function in $GF(2^{n-1})$. It is shown that $p(x) = x^{2^i} - 1$ is a bent permutation in $GF(2^n)$ provided i and n are relatively prime and n is odd. This result was used to construct the S-boxes in LOKI,

022521 ‘Cryptographic hash functions’
B Preneel, R Govaerts, J Vandewalle, *SPRC 93 pp 161 - 171*

This is a review paper on hash functions (with 75 references). It covers one-wayness and collision resistance, birthday attacks, a number of candidate functions (including constructions from block ciphers), and recent cryptanalytic work on these candidates.

022522 ‘File encryption with no known Plaintext’
M Scott, *Dublin City University report CA-1092*

The author proposes modifying the CBC mode of DES to deny an analyst any known plaintext-ciphertext pairs. The suggested method is to use as a plaintext modifier not the last cipher block, but a nonlinear combination of the last cipher block and the last plain block.

022523 ‘Periodicity Properties of $k$the Order Linear Recurrences with Irreducible Characteristic polynomial Over a Finite Field’
L Somer, *Las Vegas proceedings p 195 - 207*

The restricted period of a sequence u_i is defined as the least positive integer t such that u_{n+t} = su_n for all positive n and some nonzero field element s. Some results are proved about the restricted period of linear sequences over finite fields.

022524 ‘FFT-Hash-II is not yet Collision-Free’
S Vaudenay, *Laboratoire d’Informatique de l’Ecole Normale Supérieure report LIENS-92-17*

The modified FFT-Hash algorithm presented by Schnorr at Eurocrypt 92 is still vulnerable; attacking it can be reduced to finding a collision of a 48-bit function and so takes about 2^{24} operations. Some possible improvements are suggested.

022525 'A p-adic Lifting Lemma and Its Applications to Permutation Polynomials'
DQ Wan, *Las Vegas proceedings p 209 - 216*

The author provides a simplified proof of Cohen's theorem that all exceptional polynomials over a finite field are permutation polynomials. This is achieved by using p-adic machinery to extend Williams' proof from the large characteristic case to the general case.

022526 'On the use of reducible polynomials as random number generators'
D Wang, A Compagner, *Math. Comp v 60 no 201 pp 363 - 374*

The authors suggest employing reducible polynomials to define shift register sequences for use as random number generators. They show that the sequences produced from reducible polynomials obey Golomb's three randomness postulates 'almost' as well as sequences produced in the customary way from primitive polynomials, provided each primitive factor of the reducible polynomial produces a sequence of sufficiently large period.

022527 'New binary sequences with perfect staircase profile of linear complexity'
YX Yang, *Information Processing Letters v 46 (29/4/93) p 27 - 29*

Rueppel's generator achieves a perfect staircase profile if the first bit is dropped, ie if $m_i = 1$ for $i = 2^j - 1$ and zero otherwise.

6 Public Key Algorithms

022601 'A secure key distribution system'
N Alexandris, M Burmester, V Chrissikopoulos, Y Desmedt, *SPRC 93 pp 30 - 34*

The authors present a simple and efficient means of incorporating authentication into Diffie-Hellman. If g is the a generator of Z_p and the ith user has secret s_i, he publishes g^{s_i} as his public key; in each run of the protocol each party chooses a random r_i, send $r_i + s_i$ to the other, and forms the shared secret $K_{ij} = g^{r_i r_j}$. This is shown to be secure if Diffie-Hellman is.

022602 'Certifying Cryptographic Tools: The Case of Trapdoor Permutations'
M Bellare, M Yung, *IBM report RC 18411 (80567)*

Extra checks may be needed when using trapdoor functions to construct more complex protocols such as zero-knowledge proofs. In particular, the Feige-Lapidot-Shamir protocol is vulnerable to cheating if the parameters are chosen so that certain functions are not one-to-one (such as if an RSA public exponent is not coprime to $\phi(n)$). To prevent this kind of attack, one can add an extra step in which the underlying algorithm's parameters are certified.

022603 'An Efficient Off-line Electronic Cash System Based On The Representation Problem'
S Brands, *University of Amsterdam CWI report CS-R9323*

The author generalises the discrete log problem to an arbitrary number of generators: instead of h being represented as $g^x \pmod p$, it can be represented as $g_1^{x_1} g_2^{x_2} \ldots g_k^{x_k} \pmod p$. He shows this to be just as hard as the basic discrete log problem; but it has the advantage that relationships between the g_i of the form 'Bank A knows a such that $g_j = g_i^a$' can be used to give extra structure to signature and identification schemes. He then uses this machinery to develop a digital cash system with a number of new features: different denomination coins can be encoded easily, as can coins which can be spent up to k times; the cut-and-choose process at coin issue can be eliminated; and users can prove their innocence if a bank tries to frame them.

022604 'Symmetry and Cryptography'
M Elia, *SPRC 93 pp219 - 231*

This paper discusses the application of concepts from group theory to cryptography, and suggests that key exchange could be based on inner automorphisms of perfect groups.

022605 'New analytical results in subset-sum problems'
GA Freiman, *Discrete Mathematics v 114 (May 1993) pp 205 - 217*

The set of sums of subsets of m integers will contain an arithmetic progression of length greater than cm^2 for some constant c, provided $m \geq d\sqrt{nlogn}$ and d is another constant. Previous results of this kind had needed $m \geq d(nlogn)^{2/3}$.

022606 'Elliptic Curve Cryptosystems Immune to Any Reduction into the Discrete Logarithm Problem'
A Miyaji, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v. E76-A no 1 (1993), pp 50–54*

This paper investigates the conditions under which methods that reduce the elliptic curve discrete logarithm problem to the discrete logarithm problem are not valid.

022607 'Permutation Polynomials over Finite Fields'
GL Mullen, *Las Vegas proceedings p 131 - 151*

This is a survey article on permutation polynomials, with 120 references, which covers research published up to 1991. It raises a number of open problems, including an extension of Carlitz' conjecture. It discusses certain applications briefly, including the Cade cipher, the use of Dickson polynomials in public key cryptology, the construction of Latin squares, and work on constructing permutation polynomials in other rings (such as $Z/(m)$).

022608 'Unless modified, Fiat-Shamir is insecure'
D Naccache, *SPRC 93 pp 172 - 180*

Fiat-Shamir may be formally as hard as factoring, bit it contains a number of implicit assumptions, such as that the verifier will check that the prover's public vector components are all different. These checks are not carried out in a number of existing implementations, with the result that attacks are easy.

022609 'Finite Fields and cryptology'
H Niederreiter, *Las Vegas proceedings p 359 - 373*

The author presents an overview of cryptographic applications of finite field theory. On the public key side, he discusses systems based on decimating shift register sequences, as well as Chor-Rivest and systems based on coding theory. On the secret key side, he discusses a number of results about the linear complexity of pseudorandom sequences.

022610 'Survey of Digital Signature Schemes'
T Okamoto, K Ohta, *SPRC 93 pp 17 - 29*

This article surveys a number of digital signature schemes and compares their computational cost. It claims that only ESIGN is practical to implement on current 8-bit smartcards.

022611 'An extension to ElGamal public key cryptosystem with a new signature scheme'
S Saryazdi, *Bilkent proceedings pp 195–198*

The author proposes to make the ElGamal signature algorithm stronger by using the product of two primes instead of a single prime. Furthermore, a signature scheme based on exponential key exchange and the ElGamal system is described.

022612 'The Subliminal Channels in the US Digital Signature Algorithm (DSA)'
GJ Simmons, *SPRC 93 pp 35 - 54*

The well known subliminal channel in El-Gamal is inefficient in that it allows only $\phi(p-1)$ different messages to be sent with the p session keys, but DSA allows the entire session key to be used, and thus q different messages can be sent to a recipient who shares the sender's secret key. Furthermore, DSA allows subliminal messages to be sent to a recipient who does not share this key, and thus (unlike El-Gamal) can combine signature and subliminal functions. This can be achieved, for example, by choosing r so that the quadratic character of (r mod p) mod q with respect to some prime lying between p and q encodes a bit.

022613 'Extended Key Management System Using Complementary Exponential Calculation'
N Torii, T Hasebe, R Akiyama, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 78–87*

This paper proposes two types of key management systems that use complementary exponential calculation. To reduce the number of primes in the centre, users in the system are divided into groups, and moduli are generated for key setup both within and between groups. Master key information is issued by a trusted centre to users, who can then generate shared keys offline.

022614 Efficient multiplication algorithm over the finite fields $GF(q^m)$ where $q = 3, 5$
TK Truong, IS Reed, MT Shih, *IEE proceedings 'E' - Computers and Digital Techniques v 140 no 2 (Mar 93) pp 92 - 95*

A fast method for multiplying in fields of characteristic three and five is presented. It uses tables of square roots, and is named the babylonian algorithm after the Babylonian use of tables of squares in integer multiplication. It is suggested for use in Golay codes and discrete log cryptosystems.

022615 'Cryptography Using Complementary Subsets of Polynomials over Finite Fields'

WA Webb, *Las Vegas proceedings p 411 - 415*

The author's previous work on knapsack-type schemes based on complementing sets of integers is generalised to complementing sets of polynomials over a finite field.

022616 'Immunization of Public Key Cryptosystems Against Chosen Ciphertext Attacks'

YL Zhang, J Seberry, *University of Wollongong report 92/2*

The authors present a formal definition of adaptive chosen ciphertext attacks, and present three methods of strengthening public key cryptosystems against these attacks. One of their techniques is based in incorporating a digital signature in the text, and the other two on hash functions.

7 Computational Number Theory

022701 'Arithmetic Operations in $GF(2^m)$'
GB Agnew, T Beth, RC Mullin, SA Vanstone, *Journal of Cryptology v 6 no 1 (1993) pp 3 - 13*
This article surveys the techniques which can be used to speed up exponentiation and the calculation of inverses in fields of characteristic two. These techniques use a normal basis, in which squaring is accomplished by means of a shift and is therefore almost free; thus, for example, in $GF(2^{593})$ we can calculate a^{-1} quickly as $a^{2^{593}-2}$.

022702 'Finding suitable curves for the elliptic curve method of factorization'
AOL Atkin, F Morain, *Math. Comp v 60 no 201 pp 399 - 405*
There are plausible arguments which suggest that the elliptic curve method for factoring a composite integer N will run faster if the elliptic curves chosen always have torsion groups whose order is divisible by some prescribed small factors. The authors exhibit several infinite families of curves for which this is true, including a family for which the order is always divisible by 16.

022703 'A fast algorithm for large number division'
M Bucci, A Di Porto, *SPRC 93 pp 241 - 254*
There is no globally optimal algorithm for long division; this follows from differing flexibility requirements and data transfer considerations. Two algorithms are presented which allow division (and modular multiplication) to be implemented in hardware in such a way that the cost is proportional to the speed required; one is based on computing successive partial quotients, and the other on successive approximation of the divisor inverse.

022704 'Fast modular exponentiation'
Ö Eğecioğlu and ÇK Koç, *Bilkent proceedings pp 188 - 194*
The authors show that, when $M^{-1} \bmod N$ is supplied along with M, the binary method applied to the canonically recoded E requires $4/3(n-1)$ multiplications on the average for computing $M^E \bmod N$, where n is the number of bits in the binary expansion of E.

022705 'Efficient bit-serial multiplication in F_{q^n}'
D Gollmann, *SPRC 93 pp 232 - 240*
Arithmetic in finite fields can be optimised in hardware, but some of the constructions used are quite complex and difficult to teach. They can often be understood more easily by regarding them as dual basis systems.

022706 'A Signed Binary Window Method for Fast Computing over Elliptic Curves'
K Koyama, Y Tsuruoka, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 55–62*
This paper proposes a method of reducing the number of operations over elliptic curves. The basic operation in elliptic cryptosystems is the computation of a multiple $d*P$ of a point P on the elliptic curve modulo n, which corresponds to the computation of $x^d \bmod n$. The proposed method is based on pre-computation to generate an adequate addition-subtraction chain for multipliers d of $d*P$.

022707 'Computing in Solvable Matrix Groups'
EM Luks, *FOCS 92 pp 111 - 120*
The author presents algorithms for calculating a number of properties of a matrix group G over a finite field F. These include membership testing, which subsumes the discrete log problem in extension fields. This can be done in time polynomial in $(n + \log \mid F \mid + \mu(G))$, where $\mu(G)$ is the largest prime in $\mid G \mid$ other than $\mid F \mid$, by constructing a tower of normal subgroups.

022708 'Counting points on elliptic curves over F_{2^m}'

AJ Menezes, SA Vanstone, RJ Zuccherato, *Math. Comp v 60 no 201 pp 407 - 420*

It is possible to design a public key cryptosystem using an elliptic curve E defined over a finite field F. The system is not secure unless the order N(E) of the group of points on the curve has a large prime divisor. Schoof gave a polynomial time algorithm for computing N(E) if the field F has an odd number of elements and Koblitz showed how to apply this algorithm to the case where F has an even number of elements. The authors give an efficient implementation of Schoof's algorithm for fields F of 2^m elements, where $m \leq 155$ and E is chosen randomly.

022709 'A Modular-Multiplication Algorithm Using Lookahead Determination'

H Morita, CH Yang, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 70–77*

This paper presents a multi-precision modular multiplication algorithm which minimizes the RAM required when implementing public-key schemes in software on computers such as smart cards and PCs. The proposed algorithm avoids the problems experienced by the Montgometry algorithm by requiring only half the RAM space and no pre- and post-processing operations. The algorithm is an extension to the approximation methods that use the most significant bits and a lookahead determination method proposed by the authors.

8 Theoretical Cryptology

022801 'Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolski-Rosen Channels'
CH Bennett, G Brassard, C Crépeau, R Jozsa, A Peres, WK Wooters, *Physics Review Letters v 70 no 13 (29 Mar 1993) pp 1895 - 1899*
The authors indicate how in theory the quantum state of a physical object could be disassembled into classical and Einstein-Podolski-Rosen information, and might be transferred to another location and reconstructed. They show however that although objects could be teleported using this technique, they could not be copied.

022802 'Efficient sharing of many secrets'
C Blundo, A De Santis, U Vaccaro, *STACS 93 (Springer LNCS 665) pp 692 - 703*
Schemes to share n secrets among a set of participants are discussed from the point of view of entropy, and lower bounds on the amount of information held by each participant are proved. Such schemes are influenced by the degree of dependence among the secrets to be shared.

022803 'Cryptographic Primitives and Quantum Theory'
C Crépeau, *Physcomp 92 pp 200 - 204*
This paper considers the possible quantum cryptographic implementation of bit commitment and oblivious transfer, and surveys the literature of applications of these primitives.

022804 'Zero-Knowledge Proofs of Knowledge Without Interaction'
A De Santis, G Persiano, *FOCS 92 p 427 - 436*
The authors investigate zero-knowledge proofs where both parties share a short random string, and the only communication is from the prover to the verifier. These are formalised, and shown to exist under suitable complexity assumptions, such as quadratic residuosity. They can be used to immunise public key cryptosystems against chosen ciphertext attacks.

022805 'Threshold cryptography'
Y Desmedt, *SPRC 93 pp 110 - 122*
This article discusses the use of shadows to generate unconditionally secure threshold signatures, and the geometric interpretation of this. It also provides an overview of related research.

022806 'Unconditionally secure broadcast authentication'
Y Desmedt, M Yung, *SPRC 93 pp 106 - 109*
The authors propose a one-time signature scheme which has one signer and a number of independent verifiers, as follows: the signer's secret key is two polynomials $P(x)$ and $Q(x)$ over a finite field; each verifier gets $P(i)$ and $Q(i)$ for some i; and the message M is signed with $P(x) + MQ(x)$.

022807 'On the Structural Complexity of Sequences, Images and Automata'
B Goertzel, *Las Vegas proceedings pp 307 - 327*
The author defines the structural complexity of a binary sequence as the size of the set of its observable regularities. This is related to algorithmic information concepts, and various computable approximations are discussed. Finally, some experimental work on the clustering of cellular automaton sequences is presented.

022808 'A Uniform-Complexity Treatment of Encryption and Zero-Knowledge'
O Goldreich, *Journal of Cryptology v 6 no 1 pp 21 - 53*
Previous works on zero-knowledge proofs required that the protocol should not leak knowledge in any instance. The author weakens this, and merely requires that finding leaky instances should be infeasible. He shows that most of the theory goes across with suitable modifications.

022809 'Improving the Performance of Enciphered B^+-Trees'
T Hardjono, T Araki, T Chikaraishi, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 104–111*

This paper suggests an approach to the selective encryption of nodes in a B^+-tree and a method to substitute the plaintext search keys in order to increase the security of the tree. The method is based on structures in combinatorial block designs, and it allows for faster traversal of the tree, hence improving the overall speed of query response. It also represents a trade-off between security and performance in that the substitution method gives less security than encryption. The block design method has the advantage of requiring only a small amount of information to be kept secret.

022810 'Public Randomness in Cryptography'
A Herzberg, M Luby, *ICSI (Berkeley) report 92-068*

This paper proposes a formal definition of public random bits, and of the effort required by an adversary to invert functions and permutations which are constructed using them. Reductions are shown from weak one-way permutations to one-way permutations.

022811 'Multiple Assignment Scheme for Sharing Secret'
M Ito, A Saito, T Nishizeki, *Journal of Cryptology v 6 no 1 (1993) pp 15 - 20*

An access structure on a set P is defined to be a set of subsets of P which is upwardly closed under inclusion, ie if A is in the structure and $A \subseteq A* \subseteq P$, then $A*$ is also in P. It is shown that there exists a multiple assignment scheme satisfying any such structure. An upper bound on the number of shadows required is given; this bound is sharp when we do not have $A \subset A*$ for any A, $A*$ in the structure.

022812 'On the Complexity of Composite Numbers'
T Itoh, K Horikawa, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 23–30*

This paper introduces two kinds of subset of odd composite numbers, 1MOD4 and 3MOD4. The authors show, firstly, that there exists a four move blackbox simulation perfect zero-knowledge interactive proof (ZKIP) for the complement of 1MOD4 without any unproven assumption; secondly, that there exists a five move blackbox simulation perfect ZKIP for 1MOD4 without any unproven assumption; thirdly, that there exists a four move blackbox simulation perfect ZKIP for 3MOD4 without any unproven assumption; and lastly, that there exists a five move blackbox simulation statistical ZKIP for the complement of 3MOD4 without any unproven assumption.

022813 'On the Complexity of Constant Round ZKIP of Possession of Knowledge'
T Itoh, K Sakurai, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 31–39*

This paper investigates the round complexity of zero-knowledge interactive proofs (ZKIPs), and shows that if a relation R has a three move blackbox simulation ZKIP, then there exists a probabilistic polynomial time algorithm that on input x ourputs y such that $(x, y) \in R$ with overwhelming probability if x is in dom R, and outputs "$\perp$" with probability 1 if x is not in dom R. This result cannot be generalised to ZKIPs with more than four moves, because there exists a four move blackbox simulation perfect ZKIP for any nontrivial relation R.

022814 '5-Move Statistical Zero Knowledge'
K Kurosawa, M Mambo, S Tsujii, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 40–45*

This paper shows that, if NP language L has an invulnerable generator and if L has an honest verifier standard statistical ZKIP, then L has a 5 move statistical ZKIP.

022815 'Communication Complexity of Perfect ZKIP for a Promise Problem'
K Kurosawa, T Satoh, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 46–49*

The authors define the communication complexity of a perfect zero-knowledge interactive proof as the expected number of communication bits needed to achieve the target error probabilities. This paper shows, for a specific class of quadratic residuosity, a perfect ZKIP whose communication complexity is 11/12 of that of the standard perfect ZKIP.

022816 'A general scheme for probabilistic public key encryption'
S Lechner, *SPRC 93 pp 123 - 133*

The author shows that one could construct trapdoor predicates from any NP-complete problem which has a large family of solution-preserving polynomial time transformations. The secret key would be a solution of an instance of the problem and the public key this instance; a bit would be sent to him by means of an instance which did, or did not, share the solution.

022817 'Some Applications of Source Coding in Cryptography'
JL Massey, *SPRC 93 pp pp 143 - 160*

This article reviews five source coding techniques (Shannon-Fano, Huffman, Lynch-Davisson, Elias-Willems and Lempel-Ziv) and discusses their possible applications in cryptology. These include reducing plainext redundancy, homophonic coding, testing random number generators, and strengthening weak keystream generators.

022818 'The relevance of information theory to modern cryptography'
JL Massey, *Bilkent proceedings v 1 pp 176–182*

The information-theoretic and the complexity-theoretic approaches to cryptography are contrasted. The author argues that although the main successes in cryptography in the recent past have come about through the complexity-theoretic approach, the information-theoretic approach may have a better chance of leading to provably-secure practical ciphers. A recently developed information theoretic approach, due to Maurer, is used to illustrate the power and versatility of such techniques in cryptography.

022819 'Perfect Zero-Knowledge Arguments for NP Can Be Based on General Complexity Assumptions'
M Naor, R Ostrovsky, R Venkatesan, M Yung, *ICSI (Berkeley) Report 92-082*

The authors present a bit commitment protocol which is based on an arbitrary one-way permutation. It works as follows: the verifier sends a random, full-rank, upper triangular binary matrix whose rows are h_1, ..., h_n; the prover chooses a random n-bit vector x and uses the one-way permutation f to form $y = f(x)$; he then sends the verifier the dot product of h_i and y for $i = 1$ to $i - 1$, leaving two possible values for y; and tells the verifier whether the bit to which he wishes to commit is the statement 'y is lexicographically the smaller of these' or its negation. It is shown that any algorithm which reveals the bit after the commit stage (but before x is revealed) can be turned into an algorithm to invert f. It follows that zero-knowledge arguments can also be based on such permutations.

022820 'Filtering random noise via data compression'
BK Natarajan, Data Compression 93 pp 60 - 69

Random noise, unlike ordered information, is hard to compress; the author shows how to use an arbitrary compression algorithm to filter noise from signals. This is a generalisation of low-pass filtering, and may be viewed as an application of Occam's razor.

022821 'Practical Consequences of the Discrepancy between Zero-Knowledge Protocols and their Parallel Execution'
K Sakurai, T Itoh, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 14–22*

In this paper, the authors investigate the essential discrepancy between the serial version and the parallel version of the Fiat-Shamir scheme, and clarify the information "leaked" in the parallel version. It has been shown that the parallel version of the Fiat-Shamir scheme, unlike the serial version, is not zero-knowledge unless the factorization is tractable. The authors observed that the information leaked in the parallel version is closely related to a digital signature which is a modification of the Fiat-Shamir identification scheme, and the parallel version of zero-knowledge protocols leave a trace. The authors consider both the positive and the negative sides of the discrepancy.

022822 'The Sibling Intractable Function Family (SIFF): Notion, Construction and Applications'
Y Zheng, T Hardjono, J Pieprzyk, *IEICE Trans. on Fund. of Elec., Comm. & Comp. Sci., v E76-A no 1 (1993), pp 4–13*

This paper presents a new concept in cryptography called the sibling intractable function family (SIFF). SIFF is a generalization of the concept of universal one-way hash function family, and has the property that given a set of initial strings colliding with one another, it is computationally infeasible to find another string that would collide with the initial strings. The paper presents the various concepts behind SIFF together with a construction of SIFF from any one-way function. It also discusses applications of SIFF to practical problems including the hierarchical access control problem, the shared mail box problem, access control in distributed systems and the multiple message authentication problem.