Computer and Communications

Security Reviews

Volume 2 Number 3 September 1993

CONTENTS

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

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by 20 August 1993; and books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

Oakland 93 IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California, 24-26/5/93 *Proceedings published by the IEEE Press, Los Alamitos, CA; ISBN 0-8186-3371-0*
Franconia 93 Workshop on Foundations of Computer Security, Franconia, USA, 15-17/6/93 *Proceedings published by the IEEE Press, Los Alamitos, CA; ISBN 0-8186-3950-4*
Eurocrypt 93, Lofthus, Norway, 23-27/5/93, *Proceedings to be published in Springer Lecture Notes in Computer Science series; page numbers given here are for preproceedings*

We regret that, owing to UK copyright laws, we cannot supply copies of articles reviewed in this journal.

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

Regular subscriptions: These are £95 or \$145: send your cheque or corporate 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.

Special offer

New subscribers who order a 1994 subscription before the end of December 1993 can get volume 2 number 4 (December 1993) free of charge. Alternatively, we can supply a 1994 subscription plus a complete set of 1992 and 1993 back numbers for only 50% over the 1994 subscription price - £90 for individual subscribers and £142.50 for regular subscribers. This offer is only available while stocks last.

1 Applications and Engineering

023101 'Global thrust by prepaid SmartCash'
NR Achs, *Cards International no 89 (7/7/93) p 5*

A joint venture has been set up between smartcard maker GemPlus and terminal maker Verifone to provide an international prepaid card, which will be sold through banks and used to pay for items under $10 such as phone calls, transport tickets and vending machine items.

023102 'Smartcard update'
D Austin, *Financial Technology Insight (July 93) pp 5 - 8*

Although only France and Norway have introduced smartcards on a major scale in payment systems, there are many smaller schemes where these products are used as prepaid tokens, access control devices or even electronic wallets. Now the EC is funding a project called CAFE under its ESPRIT program to agree a requirements specification for a Europe-wide electronic wallet. This will function as a credit card, a debit card, a driving licence and an access token.

023103 'Achieving Stricter Correctness Requirements in Multilevel Secure Databases'
V Atluri, E Bertino, S Jajodia, *Proc Oakland 93 pp 135 - 147*

The concurrency control algorithm used by 'Trusted Oracle' is described; it generates histories which are only level-wise serialisable, and this might affect the database's integrity. It is shown that higher degrees of correctness can be obtained by controlling the order in which transactions are submitted to the scheduler.

023104 'Image processing would cut clearing costs'
Banking World (April 93) pp 40 - 42

Processing images of cheques rather than the actual paper could save UK banks a lot of money, provided the authentication problem can be solved. So far, courts have accepted managerial evidence that electronic documents are authentic and have not required technical evidence to be led, but it would be imprudent to rely on this. On the other hand, as cheque volumes decline, their processing costs may slip down the agenda.

023105 'Suppliers on crest of EFTPOS wave'
Banking World (June 93) p 35

The number of EFTPOS terminals in the UK has risen rapidly, thanks to the banks' policy of reducing floor limits and making authorisation calls toll-free. At the end of 1991, the UK had 190,000 terminals, or 1 per 300 population; this was second only to France, which had 203,000, or 1 per 279. This buying spree has helped UK suppliers Racal, Fortronic and ACI to build a worldwide business.

023106 'The secret radio that kept Resistance lifelines open'
C Bovill, *Electronics World & Wireless World (Sep 93) pp 772 - 776*

This article describes the S-phone, a combined UHF air-to-ground radio and direction finding unit which was used by the RAF during World War 2 to communicate with resistance groups and to target supply drops.

023107 'Security Services in ANSA'
JA Bull, AJ Herbert, *ANSA report AR.009.0 (May 1993)*

This report sets out the architectural principles for security services in ANSA. The mechanism is objects which maintain and enforce their own security policies. A hardware protected system nucleus enforces encapsulation; capsules protect sets of objects with similar security needs; guards use access control lists or access certificates to take access control decisions (and may be located either within the objects they control, or outside them but with an authenticated control path). Servers provide such security functions as object creation, naming, and authentication.

023108 'An introduction to a historic computer document - the 1946 Pendergass report - cryptanalysis and the digital computer'
C Burke, *Cryptologia v 17 no 2 (April 93) pp 113 - 123*

This presents a US Navy report ('Cryptanalytic use of high-speed digital computing machines') which showed how many important problems (such as Enigma) could be solved by computer, and convinced that organisation to fund the Atlas computer, which became operational in 1950. The report itself describes the assembly code proposed by von Neumann and gives sample programs, including one to break an Enigma by exhaustive search for wheel settings given a few guessed plaintext characters. This program was estimated to take 7 minutes to run, as against 20 minutes for a bombe; another example is of a Hagelin decryption which is estimated to take 7 seconds for a 1000 character message.

023109 'Auditing MRP systems'
T Burns, *ACM SIGSAC v 11 no 3 pp 2 - 13*

Material requirements planning systems are widely used for controlling inventory and scheduling production. The requirements for such a system to be certified 'Class A' under the relevant US industry scheme are described, and the audit opportunities are discussed. The main thrust lies in preventing and detecting programming errors which could cause waste; this involves detecting heavy use of override transactions, using inventory checks and other external reporting mechanisms, installing error trapping routines, and ensuring that data maintenance procedures are robust.

023110 'DECnet Security (Not Necessarily an Oxymoron)'
RA Clyde, *Computers and Security v 12 no 2 (Mar 93) pp 123 - 127*

This paper describes the DECnet security mechanisms and associated network objects, explains how these features should be implemented using NCP and VMS facilities, and describes some of the traps which have to be avoided.

023111 'A guide to the 5ESS'
2600 Magazine (Summer 1993) pp 4 - 11 and 32 - 34

This article provides a hackers' guide to the 5ESS, a switch used in US telephone exchanges. Its architecture, command language and maintenance channel are described, as is the mechanism by which changes are made to subscriber telephone configurations.

023112 'Self-defence for networks'
J Davies, *Financial Systems (Summer 1993) pp 35 - 38*

The author describes the use of ASIC repeater chips to construct a LAN security architecture. These chips are installed in the interface cards where they filter incoming data.

023113 'Security - The Continuing Issue'
Financial Technology Insight (July 93) p 19

At EDI conferences, security attracts more attention than any other single issue. It has a complex relationship with the contracts which underlie the EDI business. At present, however, little is actually implemented, as most EDI systems provide links between mutually trusting parties.

023114 'Crédit Lyonnais uses airline network to link to corporates'
Financial Technology International Bulletin v X no 11 (July 93) pp 7 - 8

Crédit Lyonnais has built a cash management system on top of the airline network SITA to service corporate customers worldwide. The customer uses a PC with a smartcard and PIN to send a message through SWIFT to one of the bank's servers; the requested information is sent back via SITA. Authentication and nonrepudiation services are supported.

023115 'Assuring Distributed Trusted Mach'
T Fine, SE Minear, *Proc Oakland 93 pp 206 - 218*

This article provides an overview of the origin, concepts and design of Distributed TMach. The project goal was to use the Mach 3 kernel as the base for a secure distributed computing environment, and its principal mechanism is type enforcement. As this is intransitive, it is more general than multilevel security. Security servers are used to cut the kernel complexity, and the supporting operating system semantics are described. A belt and braces approach is used, with tasks needing both 'rights' and 'permissions' to do anything; the latter are supplied by the security servers and cached in the kernel. The article concludes with a detailed description of the threat model and the proposed countermeasures.

023116 'LPI in Pulsed Laser Space Communications'
RM Gagliardi, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 673 - 678*

The author discusses the options for implementing low probability of intercept (LPI) communications using lasers, especially in space communications. Pulse position modulation is the most power efficient form of encoding, but where the intercept probability is a concern, this should be modified using techniques such as varying the wavelength and using repeated transmissions at low peak power, so that the detected pulse energy is below the detected background energy. An analysis of such communications links is presented.

023117 'The impersonal touch'
T Gandy, *The Banker (Mar 93) pp 60 - 61*

Many banks now dispense 75 - 80% of their cash via ATMs, and the next move should be self service branches. One pioneering Portuguese bank has installed cash dispensers, currency converters, touch-screen information terminals and large-screen advertising. The open question is how to sell insurance and loans; should one use interactive video, or retain a small number of staff?

023118 'Design and Cryptanalysis of Transform-Based Analog Speech Scramblers'
B Goldburg, S Sridharan, E Dawson, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 735 - 744*

Digital signal processors are used to implement analog speech scramblers based on transforming speech into a spectral domain, permuting the components, and then transforming it back into the time domain. Both fast Fourier transforms and prolate spheroidal transforms have already been reported; these are studied, together with discrete cosine transforms and Walsh Hadamard transforms, in this paper. The residual intelligibility of each method was measured empirically, and the vulnerability to vector codebook cryptanalysis was also analysed. Of the four transform techniques, the discrete cosine transform outperformed the other methods. It can be strengthened still further by inserting dummy components.

023119 'A man with grand visions'
P Harverson, *Banking Technology v 10 no 4 (May 93) pp 30 - 32*

This article profiles a businessman called Bipin Shah, who is building an ATM network in the USA with a view to offering a wider range of services, such as loans and airline ticket sales. He plans to market these through POS terminals in shops as well as through conventional ATMs.

023120 'NADIR: An Automated System for Detecting Network Intrusion and Misuse'
J Hochberg, K Jackson, C Stallings, JF McClay, D DuBois, T Ford, *Computers and Security v 12 no 3 (May 93) pp 235 - 248*

This paper describes an expert system developed at Los Alamos to streamline the review of audit trails by highlighting suspicious behaviour. It provides a brief history of previous systems, and describes how their ideas were adapted to a pre-existing, complex, multilevel network. The main effort was in parsing, rationalising, aggregating and reducing large quantities of heterogeneous audit data; thereafter, histories of user activity were built up and used as a baseline to detect anomalies. There turned out to be side benefits in identifying persistent user errors and opportunities to improve network management.

023121 'Radix-2^n multiplier structures: a structured design methodology'
MK Ibrahim, *IEE Proceeding on Computers and Digital Techniques v 140 no 4 (July 1993) pp 185 - 190*
The author surveys some of the designs used in binary multipliers, and proposes iterative multiplier arrays which require nearest-neighbour communication only, give simple pipelining, and generalise easily to other number bases.

023122 'USTAT - A Real-time Intrusion Detection System for UNIX'
K Ilgun, *Proc Oakland 93 pp 16 - 28*
The author describes USTAT, an audit trail analysis tool which uses rule-based reasoning to search for penetration attempts against unix systems. It is based on state transition analysis and it searches for the auditable activities which best characterise each penetration scenario.

023123 'A framework for the study of homophonic ciphers in classical encryption and genetic systems'
JC King, DR Bahler, *Cryptologia v 17 no 1 (Jan 93) pp 45 - 54*
The authors discuss the relation between the multiplicity and the unicity distance of homophonic ciphers, and the language statistics available to the analyst. These results are applied to molecular biology and used to plot the 'multiplicity' of a number of genes. This may lead to an application of cryptologic ideas in the design of oligonucleotide probes in biology.

023124 'A 77-year old challenge cipher'
L Kruh, *Cryptologia v 17 no 2 (April 93) pp 172 - 174*
This article contains a challenge cipher set by Mauborgne in 1915 for the US Army Signal School, and since republished elsewhere without being solved.

023125 'First principles analysis of computer information leakage'
DX Liu, WL Guo, CX Fan, *Journal of Xidian University v 20 no 2 (June 1993) pp 74 - 79 (in Chinese)*
The authors tackle the Tempest problem by analysing the output waveform and spectrum of the PC video port and of the integrated circuits on its display card. These provide the main component of the electromagnetic radiation which can lead to information leakage. The approximate spectrum of this radiation has been obtained; this is significant for studying both the techniques for intercepting this information and the methods available to prevent such attacks.

023126 'Complementarity attacks and control vectors'
D Longley, SM Matyas, *IBM Systems Journal v 32 no 2 (1993) pp 321 - 325*
The key control vectors used in the IBM 4753 and related products are implemented in such a way as to prevent the DES complementation property being used to manipulate them. This involves features which were incorporated in anticipation of the attack but not previously disclosed in the literature.

023127 'Status and Development of A-D-A Voice Cipher Technique'
ZG Ma, YL Lu, *Communications Technology and Development no 1 (1993) (in Chinese)*
This paper reviews the research status of voice cipher systems in which speech is converted to digital form, compressed, encrypted, and then converted back to analogue form for transmission. Both synchronous and asynchronous systems and their development trends are discussed.

023128 ‘Smartcards - has their time come at last?’
S Marek, *Scottish Banker (Feb 93) pp 2 - 5*

This article reviews a number of UK smartcard applications including Sky TV, British Gas, garage cards, bus ticketing and club memberships. The next move may be regional cards which enable a user to pay for a portfolio of services in one county; a scheme of this kind is just being introduced in Lanarkshire in Scotland.

023129 ‘Authentication Method with Impersonal Token Cards’
R Molva, G Tsudik, *Proc Oakland 93 pp 56 - 65*

Challenge-response authentication tokens are used to prevent various attacks on passwords, but existing devices are expensive to administer, as they are personalised for each user. The authors propose an alternative design: impersonal tokens which encrypt the time under a secret device key to give two pseudorandom numbers. A user can encrypt his PIN by adding it mentally to the first of these, and send it (with the device serial number) to a server; the server identifies itself in turn by returning the second pseudorandom number.

023130 ‘EDI in insurance’
Å Nilson, *Financial Technology Insight (May 93), pp 17 - 19*

This survey covers six different EDI networks used by insurance brokers and insurers in the UK, Belgium, France, the Netherlands and elsewhere.

023131 ‘Security Analysis of the INTELSAT VI and VII Command Network’
RL Pickholtz, DB Newman, YQ Zhang, M Tatebayashi, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 663 - 672*

This paper reports a study of the dependability of the Intelsat VI and VII telemetry, tracking, command and monitoring system. Commands are encrypted to prevent tampering, and contain a command counter to prevent replay attacks. The protocol used is modelled to study the effects of various kinds of error.

023132 ‘Detection and Elimination of Inference Channels in Multilevel Relational Database Systems’
XL Qian, ME Stickel, PD Karp, TF Lunt, TD Garvey, *Proc Oakland 93 pp 196 - 205*

The authors describe DISSECT, a tool for finding possible inference security problems in multilevel databases. These problems are detected as different series of key relationships which connect the same entities. The method is restricted to deductive properties, and excludes those properties which involve common sense (or any other information which is not explicitly encoded).

023133 ‘Secure Data Transmission in Extended Ethernet Environments’
F Recacha, JL Melús, X Simón, M Soriano, J Forné, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 794 - 803*

The authors describe DES/RSA encryption devices which provide secure islands in an ethernet, despite being connected together by an insecure backbone. They provide technical detail on how data encryption is organised, how how sessions are set up, and how keys are managed. They also describe an implementation at the Polytechnic University of Catalonia.

023134 ‘A new weapon in the fight against hackers’
F Rees, *Computer Fraud and Security Bulletin (May 93) pp 5 - 6*

STUBS is a network security product developed by the Defence Science and Technology Organisation in Adelaide, Australia, to provide secure network gateways. These operate by requiring ‘export visas’ on outgoing information; the visas are generated by secure hardware at the terminals of trusted personnel.

023135 'A Framework for Federating Secure Systems'
RTO Rees, JA Bull, *ANSA report AR.008.0 (May 1993)*

This report describes the security features of the ANSA architecture; these are designed to provide security services in distributed systems which have heterogeneous ownership and multiple security policies. The basic idea is that objects defend themselves; to achieve this, encapsulation must be enforced and interactions at interfaces must be controlled. The implications for naming, monitoring, transparency, accountability, revocation, damage limitation and the system lifecycle are discussed.

023136 'The IX Multilevel-Secure UNIX System'
JA Reeds, MD McIlroy, *AT & T Bell Labs Technical Report no 163 (1992)*

This report consists of five papers on IX, plus a glossary and manual pages. IX is a multilevel-secure variant of UNIX, aimed at research and private sector use rather than at military applications (although it does appear to draw on experience gained with B1/B2 UNIX versions). Data classification and outside communication are safeguarded; superusers are controlled by means of a privilege server; a high integrity shell is provided, as are audit mechanisms; and the rationale behind the design decisions is discussed in considerable detail.

023137 'A High-Security Microcomputer for Telecommunication Systems'
T Sato, N Kawashimo, *Hitachi Review v 42 no 3 (June 1993) pp 135 - 140*

This article describes the H8/3101 processor, developed by Hitachi for the smartcards which identify the subscriber using a GSM telephone. This has an 8-bit CPU, 10 Kbytes of ROM, 256 bytes of RAM, and 8 Kbytes of EEPROM. Each 32 byte page of EEPROM can be protected in various ways; for example, write-once protection is used to prevent overwriting attacks on PINs and keys.

023138 'Biometric identification systems update'
J Smith, *Computer Fraud and Security Bulletin (April 93) pp 6 - 8*

A number of pilot projects use biometrics to supplement or replace the passport. Frequent visitors to the US will soon be able to apply for an ID card containing their hand geometry, which will enable them to pass quickly through immigration; Canada plans trials with a similar system; Holland has been using fingerprint scanners; Germany will use both hand geometry and fingerprints; and Spain has started using dynamic signature verification.

023139 'Secure Communications by Optical Homodyne'
W Wells, R Stone, E Miles, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 770 - 777*

The authors discuss techniques for tapping optical fibre links, and present a number of techniques for preventing such attacks. These include using phase modulation with either a secret variable delay or a scrambled reference beam to cause coherence problems for an eavesdropper. They report the construction of a prototype, and quantify the residual vulnerability.

023140 'A fast multiplier based on the modified Booth algorithm'
S Sunder, *International Journal of Electronics v 75 no 2 (1993) pp 199 - 208*

The author presents an improved version of the Booth multiplication circuit, which precomputes certain partial products in order to reduce the circuit complexity.

023141 'The Authenticated Datagram Protocol: a high performance, subtransport level, secure communication protocol'
P Venkat Rangan, *Computers and Security v 12 no 3 (May 93) pp 305 - 314*

The author points out that high level authentication failures duplicate the error correction facilities at the transport layer, and proposes overlaying agent to agent communications on a secure host to host link. He reports some performance measurements for this scheme.

023142 'A New Cryptographic Key Management Scheme'

M Wang, *Chinese Journal of Computers v 16 no 2 (Feb 93) pp 106 - 112 (in Chinese)*

This paper reports a new four-level cryptographic key management scheme which is based on a secure Cryptographic Operation Kernel (COK). This supports a number of system facilities in a convenient manner, while reducing the cost and complexity of secure communications, and has been adopted by a system developer.

023143 'Automated Support for External Consistency'

JG Williams, LJ La Padula, *Proc Franconia 93 pp 71 - 81*

The authors consider how an integrity objective decomposes into user and system responsibilities. They point out that some supposed system requirements are actually user duties; and conversely, many user tasks can receive automated support, leading to systems which are more user friendly and robust. They develop a model based on the Clark-Wilson concept of enterprise integrity, and point out that the crucial factor is the mix of inputs and processes which lead to an output being warranted as correct.

023144 'Managing Secure Communications With Multilevel Security and Restricted Character Set Translation'

CA Yang, CC Tsai, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 745 - 756*

Some US Naval communications use restricted character sets, and encryption must be accomplished by character set translation rather than bit level operations. The implications of this for master key systems and for connecting with a shore-based multilevel RDBMS are discussed.

023145 'A Comparison of Password Techniques for Multilevel Authentication Mechanisms'

M Zviran, WJ Haga, *The Computer Journal v 36 no 3 (1993) pp 227 - 237*

The authors report an empirical study of the trade-off between memorability and safety of passwords. They propose that each user should have about 20 passwords which are easy to memorise, and be prompted for some subset of these by a series of questions during the logon process. If this is not feasible, the next best choice would be eight-character pronounceable passwords.

2 Operating System and Database Security

023201 'Distributed Timestamp Generation in Planar Lattice Networks'
P Ammann, S Jajodia, *ACM Transactions on Computer Systems v 11 no 5 (August 1993) pp 205 - 225*

Distributed timestamp algorithms can create covert signalling channels. A new algorithm for generating and comparing timestamps is therefore proposed; it relies on propagating time upwards from the nodes with the lowest classification, and each timestamp contains the time according to each level dominated by the entity issuing it. A message-based distributed timestamp scheme based on this is shown to be acyclic and free from deadlock.

023202 'A Model of Atomicity for Multilevel Transactions'
BT Blaustein, S Jajodia, CD McCollum, LA Notargiacomo, *Proc Oakland 93 pp 120 - 134*

The authors review the conflict between security and atomicity in multilevel database transactions (the failure of a high level write means aborting any associated low level write and thus could signal information). Two techniques for tackling this are proposed and discussed: 'low-first' which executes transactions at the lowest level upwards for as far as possible and then stops (which violates atomicity); and 'high-ready-wait' which executes provisionally top-down.

023203 'Untransferable Rights in a Client-Independent Server Environment'
J Domingo-Ferrer, *Eurocrypt 93 pp T113 - T121*

A scheme is presented under which a security server can grant sets of capabilities to clients in such a way that a client cannot transfer a subset of these to a third party; he must hand over all or none. Once clients are enrolled, extra capabilities can be granted to them publicly; but revocation entails reissuing the list of capabilities.

023204 'A shortest path network security model'
JA Fitch, LJ Hoffmann, *Computers and Security v 12 no 2 (Mar 93) pp 169 - 189*

The authors explain the risks of connecting evaluated systems together into networks, and the cascade problem in particular. They then show how to model heterogeneous networks as graphs in which each node is a locally evaluated system with a finite resistance to attack; opponents are assumed to have a finite level of resources as well, and shortest paths are used to find the least cost attacks. This model can tackle the cascade problem, and is claimed to be more efficient than Millen's matrix model, provided that the 'consumption function' which describes the attack effort required is reasonably well behaved.

023205 'Increasing Availability and Security of an Authentication Service'
L Gong, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 657 - 662*

It may be unwise to assume that an authentication server is permanently trustworthy, and in any case such servers are often a bottleneck. For these reasons, a distributed authentication service may be desirable, and a design is proposed in which a certain threshold number of compromised servers need to collude in order to break security. A number of distributed authentication protocols are presented and discussed; it is also pointed out that these could be useful to competing organisations which communicate with, but do not entirely trust, one another.

023206 'On Analysing the Bus-Contention Channel Under Fuzzy Time'
JW Gray, *Proc Franconia 93 pp 3 - 9*

The author's goal is to let users select the tradeoff between security and functionality when considering covert channels in MLS systems. It is known that if all asynchronous events are trapped by the kernel, then this kernel may add noise to any reference clock needed for a timing channel; the author considers the tradeoff between the rate of the covert channel and a legitimate requirement for an accurate clock.

023207 'On Introducing Noise into the Bus-contention Channel'
JW Gray, *Proc Oakland 93 pp 90 - 98*

A technique called probabilistic partitioning is introduced as an alternative to fuzzy time as a way to counteract the bus-contention covert channel. In this technique, randomness is introduced into the bus interrupt controller rather than the system clock. Its advantages are that it allows processes to have accurate clocks, it is more analysable, and it gives a precise tradeoff between channel capacity and performance. Its disadvantages are that it does not impede any of the other covert channels, and that it requires more custom hardware.

023208 'The Cascade Vulnerability Problem'
JF Horton, R Harland, E Ashby, RH Cooper, WF Hyslop, BG Nickerson, WM Stewart, OK Ward, *Proc Oakland 93 pp 110 - 116*

The cascade problem is discussed, and it is shown to be NP-complete (by reduction to vertex cover). An improved algorithm for detecting cascade paths is presented.

023209 'A Petri Net Representation of the Take-Grant Model'
D Marc, *Proc Franconia 93 pp 99 - 108*

The take-grant model builds access control rules from graphs and a set of rewriting rules. The author shows that Petri net techniques provide an efficient algorithm to search such a structure for all the access rights which a player can steal with the help of a given set of collaborators.

023210 'The Concurrency Control and Recovery Problem for Multilevel Update Transactions in MLS Systems'
AG Mathur, TF Keefe. *Proc Franconia 93 pp 10 - 23*

Systems that guarantee the atomicity of MLS database transactions, while allowing transaction aborts, introduce potential covert channels. The authors introduce a protocol, based on a timestamp interval for each transaction, that addresses this problem by delaying sub-transactions.

023211 'Proxy-based Authorisation and Accounting for Distributed Systems'
BC Neuman, *Proceedings of the 13th International Conference on Distributed Computing Systems (May 1993) pp 283 - 291*

The author shows that proxies can provide a powerful tool for building flexible controls in distributed systems. Restricted proxies can function as capabilities, can provide cascaded authorisation, and can be used together with access control lists to provide dual control via compound identifiers. Numbered proxies can be used as cheques. Thus the whole range of group functions, authorisation functions and accounting functions can be built up using proxy structures. Some features of this model have been implemented in Kerberos version 5, and the implementation details are described.

023212 'Interconnecting Domains with Heterogeneous Key Distribution and Authentication Protocols'
F Piessens, B De Decker, P Jansen, *Proc Oakland 93 pp 66 - 79*

The authors present proxy mechanisms for inter-domain authentication using secret key algorithms and security servers. These can be implemented in a gateway between two domains, and need not interfere in the internal security mechanisms of either; they can also cope with both peer-to-peer and client-server architectures.

023213 'Preventing Denial and Forgery of Causal Relationships in Distributed Systems'
M Reiter, L Gong, *Proc Oakland 93 pp 30 - 40*

Previously, causal relationships have been seen as a potential source of covert channels and thus as something to be prevented. However, there are other circumstances in which detecting such relationships can be important, such as in preventing various securities frauds, and the type of causality enforcement needed can vary from one application to another. The possible security goals are preventing the denial and forgery of causal relationships, and possible solutions include using trusted message switches as 'causality servers', signed timestamps, and protocols in which each player either acknowledges receipt of message n in a protocol before sending message $n+1$, or incorporates in each message a hash of all messages previously received.

023214 'Modelling Restrictive Processes That Involve Blocking Requests'
D Rosenthal, *Proc Franconia 93 pp 27 - 38*
In a client-server system, blocking times may be used to construct a covert channel. The author introduces a decomposition method to describe such a system and examines some of its properties. In particular, clients may carry out blocking reads without necessarily introducing a covert channel.

023215 'On Testing for Absence of Rights in Access Control Models'
RS Sandhu, S Ganta, *Proc Franconia 93 pp 109 - 118*
The first author's typed access matrix model had previously been extended to allow testing for the absence of an access right. Here it is shown that while this extension may have been helpful in some applications, it adds no extra power; indeed it is shown how the extension's commands can be simulated in the underlying model.

023216 'A distributed capability-based architecture for the Transform model'
RS Sandhu, GS Suri, *Computers and Security v 12 no 3 (May 93) pp 285 - 303*
There is a distinction between possessing access, being able to grant access, and being able to grant the power to grant access. This is formalised in an access model presented in this paper, which builds on the first author's Oakland 89 paper and Gong's identity based capabilities. The semantics of the 'can-create' operator are investigated, and revocation issues are discussed.

023217 'Modelling a Fuzzy Time System'
JT Trostle, *Proc Oakland 93 pp 82 - 89*
The fuzzy time technique used by DEC in the VAX security kernel randomises the period between clock ticks in order to minimise the capacity of the bus-contention covert channel. However, a scheduling channel is constructed which bypasses this countermeasure; a model is developed which can be extended to multiple hosts; and finally more secure scheduling algorithms are discussed.

023218 'A model for detecting the existence of software corruption in real time'
JM Voas, JE Payne, FB Cohen *Computers and Security v 12 no 3 (May 93) pp 275 - 283*
The authors propose that software should be designed in such a way that it could detect accidental or deliberate corruption by periodically examining snapshots of its own execution history.

3 Security Management and Policy

023301 'British Credit Holes'
2600 Magazine (Summer 1993) p 12

UK credit reference agencies file credit histories by address rather than by name. It is easy to get hold of anyone's file if you know their address; just ask for a copy of the information held on you, as allowed by the Data Protection Act, and state that you used to live at the target address.

023302 'Payment systems and risk'
P Allsopp, *Banking World (May 93) pp 22 - 24*

The author, who heads the Bank of England's payment systems division, discusses systemic risk to payment systems - the possibility that a bank failure or processing disaster could propagate payment failures throughout a national system. He argues that real time settlement is the best way to control this risk.

023303 'Redefining ATM access'
D Austin, *Banking Technology v 10 no 3 (April 93) p 16*

This article reports a seminar on 'Designing Accessible Cash Dispensers', which focussed on making ATMs easier for the disabled. The main problem is enabling blind and partially sighted people to use these machines, though wheelchair access is also a problem.

023304 'The Evolved Threat Paradigm: Look Who's Wearing the Black Hats!'
D Baker, *New Paradigms Workshop II*

The foundation for TCSEC (Trusted Computer System Evaluation Criteria) was that threats would be from outside (such as from a foreign country) and not originate directly or indirectly from inside (such as from a game containing a virus). The history of computers explains this approach; but modern threats are different from those which TCSEC envisioned. However, these criteria are still the basis for developing trusted computer systems. Future versions of TCSEC should take threats from insiders more seriously.

023305 'Accidents do happen'
G Booth, *Banking Technology v 10 no 6 (July/Aug 93) pp 41 - 42*

The London branch of the Union Bank of Finland suffered a disaster when a burst water main knocked out their UPS. A number of lessons were learned during the recovery.

023306 'Master of a growing region'
Cards International no 87 (4/6/93) pp 6 - 7

The 1993 MasterCard members' meeting for the Asia Pacific region is reported. Some of the fraud countermeasures in use are discussed, including the introduction of CVCs, and a rule that any acquirer with more than ten times the world average of counterfeit losses must bear the excess. These measures have led to significant reductions in the region's fraud figures.

023307 'Bankcard fraud'
Cards International no 86 (24/5/93) p 15

Card fraud in France dropped from Ffr703m in 1990 to Ffr683m in 1991 and Ffr533m in 1992. The French banks attribute this to the use of the PIN at the point of sale, which is facilitated by equipping all cards with chips. By comparison, other countries have seen fraud increase over the same period, by 20% per annum for MasterCard issuers and 29% for VISA issuers.

023308 'Court decides software time-locks are illegal'
A Collins, *Computer Weekly (19 August 93) p 1*

A software writer who used a time-bomb to ensure that his customers paid on time has been convicted by a magistrates' court in Scunthorpe, England, of 'making an unauthorised modification'. Under Britain's Computer Misuse Act, this is punishable by up to five years' imprisonment; but the defendant was given a conditional discharge. Industry sources are quoted as saying that such time-bombs are a common industry practice; in future, vendors who include them will be committing a criminal offence unless the customer is adequately notified of their existence.

023309 'NT$50m ATM Fraud'

Computer Fraud and Security Bulletin (July 93) p 3

A bank programmer obtained the account details and PINs of 1400 customers, and used these to withdraw NT$50m (US$2m) from banks in Taichung, Taiwan. This caused a panic among both banks and customers.

023310 'Crisis ... what crisis?'

M Cornish, E Mansell-Lewis, *Computer Weekly, July 29 1993, pp 22 - 23*

This article surveys the disaster recovery scene in the UK, and describes the experience of the Banco di Sicilia in recovering from the Bishopsgate bombing. It emphasises the importance of seeing the task as business recovery and of involving business managers rather than just IT staff.

023311 'Safe as houses'

J Costello, *Communications Networks v 10 no 7 (July 1993) pp 35 - 36*

A number of network security products are discussed, together with the reasons for purchasing encryption products. Devices which validate the addresses of network devices are cheaper.

023312 'US Survey'

C Davis, *Cards International no 87 (4/6/93) pp 10 - 15*

This survey reports the transaction figures of the top ten US card issuers and gives a number of contact names. It also has news and interviews with industry figures: MasterCard has been particularly effective in attracting new issuers, and is now catching up with VISA, largely by signing up non-banks such as General Motors. Both MasterCard and VISA are developing systems to enable their customers to pay bills, and growth in the use of debit cards is forecast.

023313 'US software firms cry foul to government encryption laws'

C Dunlap, *Computer Fraud and Security Bulletin (July 93) pp 2 - 3*

The US Software Publishers' Association found 143 non-US encryption programs available versus 133 US offerings, and argues that US export restrictions are counterproductive.

023314 'Disaster recovery today'

W Farquhar, *Computer Fraud and Security Bulletin (June 93) pp 14 - 16*

Bombings and extreme weather seem to have displaced fire and software faults as the main cause of computing disasters. Bombings in particular may lead the police to deny access to an undamaged site.

023315 'Principles of Key Management'

W Fumy, P Landrock, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 785 - 793*

The authors provide a comprehensive overview of key management issues and terminology, covering the various rôles which a central service can play, and the archival, replacement, recovery and deletion of keys. Kerberos and SPX are discussed as examples.

023316 'Interactive risk analysis'

J Gordon, *Financial Systems (Summer 1993) pp 14 - 17*

The author describes his risk analysis methodology, which uses iterative dependency modelling to search for potentially catastrophic chains of events in an organisation. Differential sensitivity analysis is used to establish which statistics have the greatest effect on overall exposure.

023317 ‘United States information systems security - a myth?’
E Heinlein, *Computer Fraud and Security Bulletin (May 93) pp 13 - 15*

There are two basic reasons why US firms have spent more money on information security than foreign firms: the defence industry, which provides the tools, and the litigious nature of US society, which ensures the need for due diligence. Regulation has also helped in some states.

023318 ‘Perceptions of computer viruses: a cross-cultural assessment’
MC Jones, KP Arnett, JTE Tang, NS Chen, *Computers and Security v 12 no 2 (Mar 93) pp 191 - 197*

The authors studied attitudes towards computer viruses among students in the USA and Taiwan. Despite the US students’ making more intensive use of computers, the Taiwanese students were about three times as likely to have actually encountered a virus. The US students had a greater theoretical appreciation of viruses, but tended to have a false sense of personal immunity, and to see virus control as the computing staff’s responsibility rather than their own.

023319 ‘Velocihackers and Tyrannosaurus superior’
ME Kabay, *Network World v 10(30):89 (26 July 93)*

The movie ‘Jurassic Park’ provides a graphic illustration of a number of well known and widespread failings in computer security management. The film portrays an incident at a theme park in which computerised security systems break down; the contributory factors are a large, poorly documented system maintained by a single person, authoritarian management which will not listen to staff complaints, bad housekeeping, and containment systems which are not fail-safe.

023320 ‘Downtime can be fatal’
S Kelly, *IBM Computer Today (July/Aug 93) pp 30 - 33*

This is a general article on disaster recovery, which discusses a number of the problems and offers a number of practical tips drawn from the London bomb experience and elsewhere.

023321 ‘Riders on the storm’
S Kelly, *IBM Computer Today (Sep 93) pp 38 - 39*

This article describes the access control systems at the UK Meteorological Office. These are based on dynamic passwords, synchronised between a Novell network and a mainframe. Their principal goal is not so much preventing intrusion as enforcing strict allocation of computational resources between departments.

023322 ‘Measuring and Modeling Computer Virus Prevalence’
JO Kephardt, SB White, *Proc Oakland 93 pp 2 - 15*

The ‘epidemic threshold’ at which the spread of a virus becomes self sustaining is reached in medical models when the contact rate β exceeds the cure rate δ. However, this has to be modified for computer viruses because software sharing is localised; it turns out that δ/β must be below some threshold value ρ which depends on the topology. The practical implication is that in addition to using virus scanners to push up the cure rate, one can adopt a strategy of inoculating all machines local to an infected one. This strategy is analysed using simulations, and it turns out that the critical success factor is the speed of the organisation’s response. Empirical data collected by IBM appear to support these conclusions.

023323 ‘Improving Public Switched Network Security in an Open Environment’
R Kuhn, P Edfors, V Howard, C Caputo, TS Philips, *Computer, August 1993, pp 32 - 35*

The increasing number and diversity of telecomms providers increases the vulnerability of the public switched telephone network to disruption, whether accidental or malicious; problems include hackers and phone phreaks, software loopholes, feature interactions and inadequate testing. This affects national security, as it could threaten the ability to maintain reliable communications during a national emergency. In the US, such emergency communications are the responsibility of the National Communications System (NCS), some of whose activities are described.

023324 'Crypto rebels'
S Levy, *Wired, May/June 93, pp 54 - 61*

This article describes the activities of the 'Cypherpunks', a group of US activists involved in making cryptography as widely available as possible, in order to guarantee individual privacy and to frustrate the wish of the US law enforcement and intelligence community to control the use of secure communications. It also gives a brief history of public-key cryptography, and reviews the current politics of cryptology, including the creation of PGP, the legal battles over declassifying old cryptanalysis manuals, the emasculation of encryption algorithms used in cellular telephones, the US key escrow proposals, and the controversy over export controls.

023325 'Status and development of A-D-A voice cipher techniques'
ZL Ma, YL Lu, *Communications technology and Development no 1 (1993) pp 49 - 52 (in Chinese)*

This paper reviews worldwide published research into systems which digitise voice before encryption, and compares the development trends of synchronous and asynchronous systems.

023326 'Review of data privacy: 1992'
W Madsen, *Computer Fraud and Security Bulletin (April 93) pp 8 - 17*

This survey covers developments in data protection law and practice during 1992. Abuses were reported in the USA (especially in relation to the presidential election), in Eastern Europe (concerning former secret police files) and the third world.

023327 'The Clipper chip saga'
W Madsen, *Computer Fraud and Security Bulletin (May 93) pp 7 - 9*

This article briefly describes the Clipper chip and the controversy which its launch has engendered, including possible conflict with the Computer Security Act and with the desire of US business to export computer security products.

023328 'Data protection in single market Europe'
W Madsen, *Computer Fraud and Security Bulletin (June 93) pp 8 - 13*

This survey covers the EC directive on personal data privacy, its history, and some possible conflicts: with US trade negotiators (who consider it to be a non-tariff barrier), with the UK Data Protection Act, with European police arrangements for data sharing under the Schengen agreements, and with the human genome project.

023329 'Testability of data security standards'
R Manning, B Szczygiel, A Harry, *NPL Report DITC 217/93*

This article discusses a number of the obstacles to producing fully verified secure systems, such as the fact that formal methods do not yet cover all types of code in a system, and the problem of validating compilers. The implications for security testing are discussed; they are particularly severe for security processors as they are often deliberately designed to be inaccessible. Realistic objectives should be set when validating security products; these might include a standardised specification system and test suite.

023330 'UK Survey'
E McCullagh, R Martin, S Coleman, *Cards International no 89 (7/7/93) pp 8 - 15*

This survey presents the 1992 transaction figures for ATM and other debit cards in Britain, together with numbers of cards in issue and contact names for the main card issuers. A a number of these issuers comment on the heavy competition and lack of profit in the merchant side of the business. Fraud losses on Switch are reported as 4p per transaction, while that on VISA's Delta is estimated at 10p. Finally, a digest of annual figures for 1982-92 is presented for VISA and MasterCard; this includes cards in issue, turnover and fraud.

023331 'Down but not out'
J Milne, *IBM Computer Today (July/Aug 93) p 34*
This article describes the Bishopsgate bombing experience of the London branch of the Banco di Sicilia. Their recovery was complicated by not having copies of paper records offsite, and particularly by not having their suppliers' phone numbers.

023332 'World trade center bombing'
M Moeller, *Financial Technology Insight (Mar 93) pp 4 - 5*
This displaced over 100,000 workers and caused 350 companies to move their operations offsite. A number of DRP firms were involved, and the biggest problems had to do with simple business logistics, such as finding documents and ferrying staff to new premises.

023333 'Risk Analysis and Management'
MG Morgan, *Scientific American (July 1993) pp 24 - 30*
This article provides a broad overview of risk management for a general scientific audience. It describes the various techniques available, such as exposure and effect studies, failure mode and effect analysis, and fault tree analysis; it also discusses various psychological effects, such as the tendency to overestimate risks which are newsworthy or which are poorly understood. Finally, it discusses the techniques involved in educating the people about risk.

023334 'Game for a change'
J Newman, *Banking Technology v 10 no 6 (July/Aug 93) pp 28 - 29*
In an interview, the secretary general of the new European Committee for Banking Standards reveals three immediate goals: to put a box in each bank which will give it access to every clearing system in Europe; to develop a Europe-wide prepaid chip card; and harmonising cheque security features. A less urgent goal is setting up a committee to study encryption.

023335 'Electronic Signature - the key to mobility'
Å Nilson, *Computer Fraud and Security Bulletin (May 93) pp 17 - 19*
This article reports a conference of the same name which was held by the EC commission in Brussels in December 92, in order to investigate how the EC could promote the development and uptake of electronic signature services.

023336 'Disaster Recovery After Downsizing'
G Norman, *Computers and Security v 12 no 3 (May 93) pp 225 - 229*
Moving systems from mainframes to a distributed environment brings with it some new risks: open systems security can be poor; the range of support services may be much reduced; and heterogeneous systems make it harder to use any one manufacturer's backup service.

023337 'Computer crime law in Italy'
S Ongetta, *Computer Fraud and Security Bulletin (May 93) pp 9 - 13*
Although Italy's first data protection law goes back to 1981, the position of computing in the criminal law is still relatively undefined. ATM card forgery accounts for most computer crime, and this is dealt with by technical measures. The author recommends that additional offences be created to cover abuses such as unauthorised access and data manipulation.

023337 'The virus threat'
TR Peltier, *Computer Fraud and Security Bulletin (June 93) pp 13 - 19*
The author describes various types of malicious code such as viruses and worms, and reviews the available technical and administrative countermeasures.

023339 ‘We Need to Think About the Foundations of Computer Security’
M Schaefer, *New Paradigms Workshop II*

Many major discrepancies between computer security needs and the facts on the ground are described, and a number of illustrative examples are given. For example, the fastest acceptable covert channel in certain applications is only 10^{-3} bits per second, but new methods allow very high rate covert channels. Also, issues such as hardware maintenance make the design of secure computers much more difficult. The usefulness of formal methods is also questioned. Finally five open problems are posed.

023340 ‘Groupware Security’
R Slade, *DECrypt v 2 no 1 (Spring 1993) pp 18 - 23*

Groupware is a term being increasingly applied to software products such as IBM’s PROFS and Lotus Notes, which enable documents to be sent back and forth by members of a group. Despite the new terminology, many of the insecurities are old ones. Furthermore, as such products are highly packaged, it is hard to find out details of authentication mechanisms (if any), and whether deleted files are actually recoverable - as Oliver North found to his cost. The standard of security on offer varies greatly from one vendor to another.

023341 ‘Insurance and contingency planing: making the mix’
P Sommer, *Computer Fraud and Security Bulletin (July 93) pp 5 - 11*

Striking the right balance between technical recovery measures and insurance is a complex business, and indeed the recovery plan should be a key input to the insurance negotiation. The author provides an insurance checklist and discusses the insurer’s perspective on recovery planning.

023342 ‘Information Security in Workstation Environments’
SH Stahl, *Computers & Security v 12 no 2 (Mar 93) pp 117 - 122*

This paper discusses some of the ways in which distributed workstation environments are harder to secure than mainframes. It also lists some evaluated workstation and LAN products, and discusses the application of smartcards and Kerberos.

023343 ‘A question of identity’
M Weston, *Financial Systems (Summer 1993) pp 78 - 80*

Poor control of login passwords has been implicated in the recent case between Virgin and British Airways, and in a spate of small fraudulent claims by staff at an insurance company. Banks may also be at risk.

023344 ‘How to implement and end-to-end security framework’
K Wong, *Computer Fraud and Security Bulletin (July 93) pp 11 - 13*

This article provides a basic checklist for the items a commercial security survey should cover, and emphasises the importance of promoting consistent best practice throughout an organisation.

4 Formal Methods and Protocols

023401 'Information Flow Control in a Parallel Language Framework'
JP Banâtre, C Bryce, *Proc Franconia 93 pp 39 - 52*
The authors use CSP to describe a system with a fixed number of processors. Every variable is assigned a security level, and information flow is deduced. Phantom messages, where the lack of a message causes flow of information, are considered. The authors suggest that these rules of flow are too strong and invite further discussion.

023402 'Abstract Machines for Communications Security'
P Bieber, N Boulahia-Cuppens, T Lehmann, E van Wickeren, *Proc Franconia 93 pp 137 - 146*
The authors report using an existing formal software method, 'B-Toolkit': security properties were obtained as part of a routine verification of functional correctness. A modular approach was taken; it combined separate models of the communication channel and the cryptographic functions, which were seen externally as envelopes.

023403 'Systematic Design of a Family of Attack-resistant Authentication Protocols'
R Bird, A Herzberg, PA Jansen, S Kutten, R Molva, M Yung, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 679 - 693*
The authors characterise an authentication protocol's history as being error-free if all of the runs accepted by the two parties match one-to-one. They describe various attacks on challenge-response protocols, and discuss several protocols which have been implemented by IBM.

023404 'Formal Methods in Safety-Critical Systems'
J Bowen, *Oxford University Computer Laboratory Report*
The author surveys a large number of standards relating to safety critical systems in the military, aviation, nuclear and railway industries, and highlights those which allow or mandate the use of formal methods in software development. Two organisations whose standards insist on formal methods are the UK Ministry of Defence and Canada's Atomic Energy Control Board. Other government and industry initiatives are also discussed.

023405 'Security Structures Using Formal Methods'
C Boyd, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 694 - 701*
The author develops formal machinery in Z to analyse the confidentiality and authentication properties of secure channels, and uses it to study key exchange messages as state transitions which add new secure channels to a model.

023406 'Limitations of Logical Analysis of Cryptographic Protocols'
C Boyd, WB Mao, *Eurocrypt 93 pp T88 - T96*
The authors point out two possible pitfalls in idealising cryptographic protocols for logical analysis, and illustrate them in the case of Otway-Rees. Formal analysis should make explicit the checks done on accompanying plaintext; alternatively, protocols can be made robust by including the participants' names.

023407 'A Logical Formalisation of Secrecy'
F Cuppens, *Proc Franconia 93 pp 53 - 62*
Cuppens contrasts explicit permission with explicit prohibition, and suggests that explicit permission should be a requirement for information flow in a MLS system. Modal logic is used to define secrecy and a non-disclosure property is described; systems may satisfy this property yet still leak information, however the technique can describe a number of forms of leakage.

023408 'A Logical Analysis of Authorised and Prohibited Information Flows'
F Cuppens, *Proc Oakland 93 pp 100 - 109*

Information flow policies can be based on explicit permissions or explicit prohibitions, and an epistemic logic is developed to describe the information which an individual may know in either case. It turns out that causality can be derived from the permissions model, while the prohibitions model yields both noninterference and nondeducibility. The relative utility of the two approaches is discussed in the context of polyinstantiation, and the former seems to be preferable provided certain consistency conditions are met.

023409 'Standards and conformance testing in data security: Results of initial programme of investigation'
Data Security Group, NPL *NPL Report DITC 218/93*

This publication reports a survey of security standard testing. It considers how formal methods can be used to improve security standards at a broad range of levels, from the architectural overview down to the algorithm detail. The potential benefits of formal methods are faster implementation and more thorough testing; the main problems are their inability to describe implementation specific features such as exception handlers, and the difficulty which most users experience when trying to understand formal specifications.

023410 'Variations on the Themes of Message freshness and Replay'
L Gong, *Proc Franconia 93 pp 131 - 136*

The author discusses the use of timestamps, counters, random numbers and pseudorandom numbers to thwart replay attacks, a number of which are discussed. The choice of method depends partly on whether the freshness is to be guaranteed by the prover or the verifier; and in some cases it may be simpler to use other methods such as having different formats for outgoing and incoming messages.

023411 'Protecting Poorly Chosen Secrets from Guessing Attacks'
L Gong, TMA Lomas, RM Needham, JH Saltzer, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 648 - 656*

The authors show how offline password guessing attacks can be carried out against a number of systems, including Kerberos and SunOS Secure NFS. The way to prevent such attacks is to ensure that password guesses can only be verified by interaction with an online authentication server. A number of protocols are presented which have this property and which use either symmetric or asymmetric cryptography. Finally, the authors discuss the design principles of such protocols, together with methods for finding guessing attacks on existing protocols.

023412 'A Lattice of Information'
J Landauer, T Redmond, *Proc Franconia 93 pp 65 - 70*

The authors describe a lattice model to characterise information flow. They suggest that this model may be useful when trying to solve the aggregation problem, and show some possible conclusions one might draw from such a lattice.

023413 'Towards Formal Analysis of Security Kernels'
WB Mao, C Boyd, *Proc Franconia 93 pp 147 - 158*

The authors discuss an active attack on Otway-Rees which depends on its using a message implicitly as a nonce, and is not detected by the BAN logic. A variant of this logic is proposed in which stronger typing prevents messages and nonces from getting mixed up. A strengthened version of Otway-Rees is presented, and the new logic is used to demonstrate its soundness.

023414 'The Formal Specification of Safety Requirements for Storing Explosives'
P Mukherjee, V Stavridou, *Formal Aspects of Computing v 5 no 4 (1993) pp 299 - 336*

The authors report a project to validate the safety requirements of the UK Ministry of Defence's next generation ammunition control system to Defence Standard 00-55 using VDM. This system must prevent any magazine or vehicle having more than its rated quantity of explosive, or a dangerous combination such as detonators and explosives together. The resulting formal specification was then turned into a prototype system, and the exercise uncovered a number of contradictions and omissions in the UN regulations for the transport of dangerous goods. The specification was also useful in procedure debugging, site planning, improving communications between customers and contractors, minimising the likelihood of certain types of error, and making the safety requirements better understood.

023415 'Protocol Design for Integrity Protection'
SG Stubblebine, VD Gligor, *Proc Oakland 93 pp 41 - 53*

The authors propose a design method for secure message protocols which is based on a state-transition model, and proceeds from the security policy via the protocol constraints to derive the properties required of the encryption algorithm.

023416 'A Logical Language for Specifying Cryptographic Protocol Requirements'
P Syverson, C Meadows, *Proc Oakland 93 pp 165 - 177*

This paper proposes a formal requirements language for cryptographic protocols, in which the system's goals and assumptions can be stated unambiguously. Its assumptions and its interaction with the NRL protocol analyser are described, and a worked example is given.

023417 'A New Method for Analysing the Security of Cryptographic Protocols'
MJ Toussaint, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 702 - 714*

The author develops a formal model based on representing the knowledge of system participants as a function of their position on the protocol execution tree. This is called a 'cryptoalgebra', and is defined as the quotient of a free algebra by a set of encryption/decryption relations. It is intended to model the reasoning of a participant or attacker, and is applied to Kerberos and X.509.

023418 'A Semantic Model for Authentication Protocols'
TYC Woo, SS Lan, *Proc Oakland 93 pp 178 - 194*

Many flaws in authentication protocols could be avoided by ensuring two properties, namely correspondence and secrecy. The former means that the two parties' messages proceed in lockstep, and it quite distinct from the latter. A formal semantic model for these properties is proposed.

023419 'Trust Relationships in Secure Systems - A Distributed Authentication Perspective'
R Yahalom, B Klein, T Beth, *Proc Oakland 93 pp 150 - 164*

This paper provides a formalism for dealing with trust in an authentication chain. It suggests that there are seven kinds of trust involved: an authority can be trusted to keep secrets, to generate good keys, to identify users, to not interfere with traffic, to maintain synchronised links, to execute protocols correctly, and to provide valid references about the trustworthiness of third parties. This machinery is then used to evaluate Kerberos, SFX and SELANE.

023420 'What are the Foundations of Computer Security? : Introduction to Panel Discussion'
ME Zurko, *Proc Franconia 93 pp 85 - 93*

In this document, the four Franconia panellists (Bob Morris, John McLean, Janathan Millen and Marv Schaefer) present brief CVs and their positions on the foundations of computer security. In addition, McLean traces the development of various ideas over the last five years, and Schaefer highlights some problems which technological advance pose for the formal methods community.

5 Secret Key Algorithms

023501 'Faster attack on certain stream ciphers'
RJ Anderson, *Electronics Letters v 29 no 15 (22 July 1993) pp 1322 - 1323*
The use of low weight connection polynomials in shift-register based stream ciphers not only makes them more vulnerable to correlation attacks, but can make faster reconstruction attacks possible as well. This is shown using the multiplexer generator as an example.

023502 'A chosen plaintext attack on an adaptive arithmetic coding compression algorithm'
H Bergen, JM Hogan, *Computers and Security v 12 no 2 (Mar 93) pp 157 - 167*
A proposed encryption scheme had been based on arithmetic coding: a secret prefix would be used to put the frequency table into an unpredictable state. The authors show that this proposal can be attacked by sending a large number of plaintext symbols to reset the table into ASCII order.

023503 'On Almost Perfect Nonlinear Permutations'
T Beth, CS Ding, *Eurocrypt 93 pp M63 - M74*
The authors define measures of local and global nonlinearity for Boolean functions, and obtain several results which characterise functions with a high degree of nonlinearity. They next show how to construct highly nonlinear functions, and discuss a number of these which have (or can be transformed by a basis change into) the form X^k for various k. Some of these also possess high nonlinear order.

023504 'New Types of Cryptographic Attacks Using Related Keys'
E Biham, *Eurocrypt 93 pp W124 - W134*
This paper explains the rôle of key scheduling in block ciphers; if the means whereby the current subkey is calculated from previous subkeys does not change from round to round, then two specialised attacks may become possible. One is a chosen plaintext attack which looks for characteristics which are independent of the number of rounds, and the other, a 'chosen key' attack, involves getting plaintext encrypted under the target key K and also under $K \oplus \delta$ for some difference δ.

023505 'Two new classes of bent functions'
C Carlet, *Eurocrypt 93 pp M75 - M85*
The author considers a spectral transformation of Dillon which preserves bentness, and in particular its invariant subspace decompositions. This leads to two new classes of bent functions over $GF(2)^n$ for n even.

023506 'The M209 cipher machine'
RF Churchhouse, *IEE Review v 39 no 4 (July 93) pp 173 - 175*
The author provides an overview of the Hagelin M-209 cipher machine, and describes how to solve it in the nonoverlapped case by a superposition attack.

023507 'Boolean functions satisfying higher order strict avalanche criterion'
TW Cusick, *Eurocrypt 93 pp M86 - M95*
The author adapts the techniques of finite group theory to the study of Boolean functions. By counting the orbits containing particular functions under the action of the symmetric group, he characterises functions satisfying the strict avalanche criterion of order $n-4$ and estimates their numbers; he also gets a simpler derivation of the known results for $n-3$.

023508 'Resynchronisation Weaknesses in Synchronous Stream Ciphers'
J Daemen, R Govaerts, J Vandewalle, *Eurocrypt 93 pp T9 - T17*

The authors define stream ciphers to be key-secure if the cheapest way of predicting the keystream, given knowledge of some of it, involves determining all of the key. They use this concept to examine the case where an attacker can request resynchronisation with a chosen message key. Certain stream ciphers, such as the multiplexer generator, may be vulnerable to such attacks if the base key and message key are combined in a linear way.

023509 'The breaking of the AR hash function'
IB Damgård, LR Knudsen, *Eurocrypt 93 pp W13 - W21*

A DES-based hash function used by German banks is shown to be breakable with much less effort than brute force. This is due to one of the fixed keys used being a weak key; finding collisions is trivial, and one can even find strings which restore the initial state and can thus be prefixed to any message without changing its hash. Two such strings are exhibited.

023510 'Collisions for the compression function of MD5'
B den Boer, A Bosselaers, *Eurocrypt 93 pp W22 - W32*

Six changes were made to MD4 in order to get MD5; four were in response to the attacks of Merkle and den Boer, and the other two were thought to strengthen the algorithm. However, both of these actually weakened it: using trigonometric constants allows the addition formulae to be applied, and adding in the result of the previous step makes it easier to search for collisions. As a result, a collision in the compression function is exhibited in which the same message, with two different input buffers, compresses to the same output buffer.

023511 'An efficient computer algorithm for the calculation of the Walsh transform for incompletely specified multiple-valued binary functions'
BJ Falkowski, I Schäfer, MA Perkowski, *International Journal of Electronics v 75 no 2 (1993) pp 163 - 175*

The authors extend their previous work on using sets of cubes to determine the spectral representations of functions from $GF(p_1) \otimes GF(p_2) \otimes \ldots GF(p_k)$ to {0, 1, -} where '-' means 'don't care'. They also discuss the practical aspects of computing these spectra.

023512 'Blind Synchronisation of M-sequences with Even Span'
RA Games, JJ Rushanan, *Eurocrypt 93 pp T18 - T29*

The authors present a time-space tradeoff for correlation attacks on sequences which have an even span, or which can be factored in some other way. The attack involves processing an array of shifted sequences, and using shift estimates to home in on the phase of the target sequence. Theoretical and empirical estimates of the algorithm's running time are given.

023513 'On the Linear Complexity of Products of Shift Register Sequences'
R Göttfert, H Niederreiter, *Eurocrypt 93 pp T2 - T8*

The theory of products of shift register sequences is generalised to the case of multiple roots. In the nondegenerate case, where the two sequences have polynomials f and g with r and s distinct roots respectively, the roots of the product sequence's minimal polynomial are just the products of the roots of f and g with the appropriate multiplicities, while the linear complexity is given by deg f deg g - (deg f - r)(deg g - s).

023514 'Cryptanalysis of tree-structured substitution-permutation networks'
H Heys, S Tavares, *Electronics Letters v 29 no 1 (7 Jan 1993) pp 40 - 41*

The authors adapt Anderson's tree functions attack to break Kam and Davida's substitution-permutation networks by constructing an equivalent network of truth tables. They present an optimisation which reduces the number of chosen plaintexts required from $O(n^2)$ to $O(n)$.

023515 'An algorithmic solution of sequential homophonic ciphers'
JC King, DR Bahler, *Cryptologia v 17 no 2 (April 93) pp 148 - 165*

A ciphertext-only method of detecting homophones in a substitution cipher is presented. It assumes that the homophones for a particular symbol are used sequentially, and so all of them will be found between two occurrences of the same ciphertext symbol. It then proceeds to construct and evaluate candidate homophone sets.

023516 'Primitive Polynomials and m-sequences over GF(q^m)'
JJ Komo, MS Lam, *IEEE Transactions on Information Theory v 39 no 2 (March 1993) pp 643 - 647*

The authors show that an m-sequence over $GF(q^m)$ can be viewed as a vector whose components are shifted sequences over $GF(q)$. They determine the amount of shift and the relationships between the associated polynomials, and deal with both decimation and basis change.

023517 'Linear Recurrence Sequences over Galois Rings'
AS Kuzmin, AA Nechaev, *Uspeki Matematicheskikh Nauk (1993) pp 167 - 8 (in Russian)*

The authors prove upper and lower bounds for the linear complexity of sequences generated by linear recurrence relations over Galois rings; the lower bound in particular is better than that previously shown by Dai and Gollmann. They also give examples of cases where these bounds give good estimates of the complexity.

023518 'The two-message problem in the Hill cryptographic system with unknown cipher alphabet'
J Levine, R Chandler, *Cryptologia v 17 no 1 (Jan 93) pp 1 - 30*

The authors continue their work on solving the Hill cipher given two ciphertexts corresponding to the same plaintext under two different keys. The general problem, where the cipher alphabet is unknown, is solved using matrix algebra, and a practical worked example is given.

023519 'Linear Cryptanalysis Method for DES Cipher'
M Matsui, *Eurocrypt 93 pp W112 - W 123*

This paper presents an attack on DES, which, like differential cryptanalysis, requires about 2^{47} known plaintexts, but which uses a different approach, namely linear approximation of the S-boxes. Using this system, 8-round DES is breakable with 2^{21} known plaintexts, and various other attacks are discussed including ciphertext-only attacks on ASCII plaintext.

023520 'The use of genetic algorithms in cryptanalysis'
RA Matthews, *Cryptologia v 17 no 2 (April 93) pp 187 - 201*

The author presents a genetic system for solving simple transpositions. Candidate column orders are assessed for fitness using digram frequencies, and the best of them are used to breed a new generation of candidates, using column rotations and swaps as mutation operators. The algorithm was useful at finding partial anagrams to aid manual solution.

023521 'On the Security of the IDEA Block Cipher'
W Meier, *Eurocrypt 93 p W102 - W111*

An attack is presented on a two-round version of IDEA; it depends on a partial distributive law which holds between two of its operations, namely addition mod 2^{16} and multiplication mod $2^{16}+1$, for a proportion of operands which is significantly higher than would be the case for two random operations.

023522 'A nonlinear random number generator with known key length'
DW Mitchell, *Cryptologia v 17 no 1 (Jan 93) pp 55 - 62*

The author proposes using the decimal expansion of a rational number in a keystream. If this number is constructed as $p_1/q_1 + p_2/q_2 + \ldots$, then any desired lower bound on the cycle length can be satisfied.

023523 'Differentially uniform mappings for cryptography'
K Nyberg, *Eurocrypt 93 pp M54 - M62*
Boolean functions are defined to be differentially δ-uniform if, for any input change, the average probability of any given output difference over all the keys is bounded by δ. The degree of uniformity of a number of mappings, including $x \rightarrow x^{2^k+1}$, $x \rightarrow u^x$ and $x \rightarrow x^{-1}$, is investigated.

023524 'The inclusion-exclusion principle and its application to cryptography'
L O'Connor, *Cryptologia v 17 no 1 (Jan 93) pp 63 - 79*
The author shows how the inclusion-exclusion principle can be used to count Boolean functions which are partially linear, which have degenerate algebraic normal forms, or which satisfy the strict avalanche criterion. He also obtains estimates of the number of linear and degenerate permutations.

023525 'On the Distribution of Characteristics in Bijective Mappings'
L O'Connor, *Eurocrypt 93 pp W89 - W101*
The author shows that if S-boxes are random permutations on 2^m objects, the maximum entry in the XOR table should be 2m and the fraction of this table which is zero should be $e^{-1/2}$. It follows that, even if a block cipher has a very simple structure, we can make it arbitrarily resistant to differential cryptanalysis by making its S-boxes big enough.

023526 'How to find and avoid collisions for the knapsack hash function'
J Patarin, *Eurocrypt 93 pp W33 - W45*
The author's previous attack on Damgård's knapsack hash function used a lot of memory; in this paper, a way is shown to avoid this at the expense of more computation. In addition, a modified knapsack hash function is proposed which resists the attacks in question.

023527 'Dependence sets and functional decomposition of boolean functions'
D Patel, T Łuba, *International Journal of Electronics v 75 no 2 (1993) pp 177 - 198*
The authors present decomposition algorithms based on representing a boolean function by a family of partitions over the set of minterms. They report experimental results obtained while using these algorithms to simplify logic designs.

023528 'An automated approach to solve simple substitution ciphers'
RS Ramesh, G Athithan, K Thiruvengadam, *Cryptologia v 17 no 2 (April 93) pp 202 - 218*
The authors claim the best automatic substitution cipher solver so far - it can crack messages of 160 characters without word boundary information. Patterns such as *aba*, *abba*, and *ab?ab* are used to select candidate plaintext words from a 14,000 word English dictionary; these are then evaluated for fitness by consistency tests and by multigram frequency analysis.

023529 'On Constructions and Nonlinearity of Correlation Immune Functions'
J Seberry, XM Zhang, YL Zheng, *Eurocrypt 93 pp T30 - T48*
The authors show how to use Hadamard matrices to construct the correlation immune functions of Carlet et al, and use this construction to calculate these functions' algebraic degrees, nonlinearity and propagation characteristics. They also show how to combine correlation immune functions using Kronecker products.

023530 'Use of a genetic algorithm in the cryptanalysis of simple substitution ciphers'
R Spillman, M Janssen, B Nelson, M Kepner, *Cryptologia v 17 no 1 (Jan 93) pp 31 - 44*
The authors report using a genetic algorithm to solve monoalphabetic substitutions. Randomly chosen keys were evaluated for fitness using letter and digram frequencies, and the fittest candidates were then 'mated' and subjected to mutation to provide the next generation of keys. The 'mating' operation used a selective crossover, in which the 'best' character of each key was passed on.

023531 'Effective Methods of Preventing the Attack of Differential Cryptanalysis'
CJ Tang, *Journal of the National University of Defense Technology v 15 no 1 (1993) pp 1 - 6 (in Chinese)*

This paper gives an overview of differential attacks on block ciphers and analyses the principles behind these attacks. It presents seven methods which can be used to increase the resistance of ciphers such as DES to these attacks.

023532 'Polyphase Sequences with Low Autocorrelation'
N Zhang, SW Golomb, *IEEE Transactions on Information Theory v 39 no 3 (May 1993) p 1085 - 1089*

The authors define Golomb sequences, which can be constructed for any integer period length L. They prove that these have perfect in-phase autocorrelation, and that their out-of-phase autocorrelation is bounded by $\sqrt{L/3}$.

6 Public Key Algorithms

023601 'An Implementation of Elliptic Curve Cryptosystems Over $F_{2^{155}}$'
GB Agnew, RC Mullin, SA Vanstone, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 804 - 813*

The authors provide a brief tutorial on elliptic curve cryptosystems and on the use of normal bases in finite fields. They then describe implementing an elliptic curve system over $GF(2^{155})$ which uses normal basis multiplier hardware to do the field calculations, and achieves a throughput of 60 Kbit/sec.

023602 'Practical RSA trapdoor'
RJ Anderson, *Electronics Letters v 29 no 11 (27 May 1993) p 995*

The author proposes making Piper's trapdoor more practical by choosing RSA modulus primes from an arithmetic sequence. Such a booby-trapped modulus can be factored more easily by anyone knowing the parameters of the sequence.

023603 'Integrating a key distribution procedure into the digital signature scheme'
B Arazi, *Electronics Letters v 29 no 11 (27 May 1993) pp 966 - 967*

The Diffie-Hellman and DSA algorithms can be combined to give an authenticated key exchange: A sends B the message $m = g^u \bmod p$ and $s = k^{-1}[h(m) + xr] \bmod q$, B sends A a similar message with $m = g^v \bmod p$, and the two parties can then use the Diffie-Hellman key g^{uv} to communicate.

023604 'Fully-fledged two-way public key authentication and key management for low-cost terminals'
MJ Beller, Y Yacobi, *Electronics Letters v 29 no 11 (27 May 1993) pp 999 - 1001*

The authors present a key exchange and authentication protocol based on Rabin and El-Gamal, in which one of the players needs only two modular squarings per protocol run.

023605 'Distance Bounding Protocols'
S Brands, D Chaum, *Eurocrypt 93 pp W70 - W88*

The authors point out that middleperson attacks on zero knowledge identification schemes can be prevented by making the response fast enough: the distance between the prover and verifier is then bounded by the distance which light can travel in that time. Protocols can be constructed in which calculating the response to a challenge requires very few gate delays, and thus the verifier can be sure that the prover is situated within a few feet of him; these protocols can also be applied to wallets with observers.

023606 'Master keys for an M^3 cryptoscheme'
CC Chang, RJ Hwang, *Cryptologia v 17 no 2 (April 93) pp 175 - 186*

The authors show that a system which they proposed previously - an adaptation of Rabin encryption from a quadratic to a general cubic function over a finite field - can have a master key which will perform any user's secret key operation.

023607 'A New Generalised Group-Oriented Cryptoscheme Without Trusted Centers'
CC Chang, HC Lee, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 725 - 729*

Group oriented cryptosystems should enable the sender of a message to specify a number of combinations of members of the recipient group who can decrypt it. The secret sharing scheme of Lin and Harn is adapted to provide this functionality.

023608 'Improved Privacy in Wallets with Observers'
RJF Cramer, TP Pedersen, *Eurocrypt 93 pp W58 - W69*

The authors consider how to guarantee that electronic wallet transactions will remain secure, even if the wallet is opened at some later time. They show that common coin flips can be used between the observer and the outside world as identifiers, but that the observer's and validator's views of these can be kept statistically independent in order to prevent any breakdown of privacy.

023609 'A new elliptic curve analogue of RSA'
N Demytko, *Eurocrypt 93 pp M39 - M48*

The author proposes a public key scheme based on an 'elliptic curve' over Z_n where n is composite and its factorisation is kept secret. This scheme can be used in the same modes as RSA, but appears to be resistant to homomorphism attacks.

023610 'Generating RSA keys without the Euclid algorithm'
MFA Derôme, *Electronic Letters v 29 no 1 (7 Jan 1993) pp 19 - 21*

Where $s = (p-q)(q-1)/2$, the RSA secret key corresponding to a public key of exponent e=3 and modulus pq can be calculated simply as $d = (s+1)/3$ where $s \equiv 2 \pmod 3$ and $d = s-(s-1)/3$ for $s \equiv 1 \pmod 3$. Similar formulae can be obtained for larger public exponents.

023611 'Single term off-line coins'
N Ferguson, *Eurocrypt 93 pp W46 - W57*

A more efficient way to construct electronic cash is presented; there is no need in this scheme for a cut-and-choose protocol at coin issue, and the coins are compact in both storage and computational terms, requiring about 250 bytes each to store and 32 modular multiplications to spend. Nonetheless, the coins remain unconditionally private unless spent more than once.

023612 'ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution'
L Harn, SB Yang, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 757 - 760*

The authors propose an ID-based system which uses Agnew's signature scheme to calculate, for each member ID_j, public and secret numbers r_j and s_j such that $\alpha^{ID_j}/r_j^{-r_j} \equiv Y \pmod p$, where α is a common generator of Z_p^*, and Y is the centre's secret key. This means that two parties can use $Y^{s_i s_j}$ as a secret key; it is equal to $(\alpha^{ID_j} r_j^{-r_j})^{s_i}$ and $(\alpha^{ID_i} r_i^{-r_i})^{s_j}$. However it does not work offline, as the two parties must exchange (ID_i, r_i) and (ID_j, r_j) during key setup.

023613 'Anderson's RSA trapdoor can be broken'
BS Kaliski, *Electronics Letters v 29 no 15 (22 July 1993) pp 1387 - 1388*

The author shows that Anderson's proposed RSA trapdoor can be detected using lattice basis reduction, and that 'trapped' moduli can be factored for certain sizes of the parameters.

023614 'Fast Server-Aided Secret Computation Protocols for Modular Exponentiation'
S Kawamura, A Shimbo, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 778 - 784*

Four different server-aided RSA signature protocols are presented, which are based on different ways of organising the exponentiation, and the amount of multiplication, communication and memory required is calculated in each case.

023615 'A new public-key cryptosystem'
E Kroup, *Proceedings of 5th Swedish-Russian Workshop on Information Theory (to appear)*

A new cryptosystem is suggested, based on McEliece's. The public key is a pair (G^*, Q) for $G^* = P_k GM$, where P_k is a k by k permutation matrix, G is the generator matrix of a Goppa code, $M = Q/P$ is an invertible n by n matrix, Q is an l by n matrix, and P is an n by l matrix.

The secret key is the matrices G, $P-k$ and P; the main difference from McEliece's system is that an error in encryption has the form ϵQ where ϵ is an l-tuple of bounded weight.

023616 'Algorithmic measures for preventing the middleperson attack in authentication schemes'

CH Lim, PJ Lee, *Electronic Letters v 29 no 14 (8 July 1993) p 1281*

The authors propose three ways of immunising Schnorr's identification scheme against middleperson attacks. These involve binding either the verifier's identity or public key in the prover's initial message, or binding his identity into the challenge which he sends in the second message.

023617 'Can OSS be Repaired?'

D Naccache, *Eurocrypt 93 pp T82 - T87*

Two variants of the Ong-Schnorr-Shamir signature scheme are presented in which the Pollard-Schnorr attack is prevented; one adds internal redundancy to the signature, and the other introduces nonlinearity.

023618 'On Key Distribution and Authentication in Mobile Radio Networks'

C Park, K Kurosawa, T Okamoto, S Tsujii, *Eurocrypt 93 pp T131 - T138*

A key distribution protocol presented at Crypto 89 by Tatebayashi and others is shown to be insecure once it has been run three times, even if messages are timestamped. A modified protocol is proposed to replace it.

023619 'Subliminal Communication is Easy Using the DSA'

GJ Simmons, *Eurocrypt 93 pp T65 - T81*

The author continues the discussion of subliminal channels in the digital signature algorithm. He focusses in this paper on the broadband channel - the one which requires the recipient to know the sender's secret key, and uses examples to compare it with the similar channel in the standard El-Gamal signature scheme. He concludes that DSA provides the best subliminal channels so far discovered.

023620 'An Introduction to the Mathematics of Trust in Security Protocols'

GJ Simmons, *Proc Franconia 93 pp 121 - 127*

The author discusses two problems with proxy mechanisms. The first is how these can be implemented safely if one is compelled to use an algorithm such as DSA which has covert channels. His solution is to choose the message key by negotiation with a third party such as a gatekeeper, in such a way that the gatekeeper can check that the agreed message key was used but cannot find out the key's actual value. The second is that when you trust someone, you trust everybody whom they trust; the author shows how to use access structures to deal formally with this problem.

023621 'Weaknesses of a public-key cryptosystem based on factorisations of finite groups'

J Stern, *Eurocrypt 93 pp M49 - M53*

A weakness is shown in the public key system proposed by Qu and Vanstone at Auscrypt 92. This was a kind of trapdoor knapsack; the attack uses its matrix representation, in which the grouping of certain rows and columns leaks information about the secret key.

023622 'A new scheme of non interactive ID-based key sharing with explosively high degree of separability'

S Tsujii, K Araki, T Sekine, *Tokyo Institute of Technology report 93TR-0020*

Previous non-interactive ID-based key sharing schemes have all suffered from the problem that members can collude to recover the centre's secret. A new scheme is proposed in which random numbers are added to member secrets in order to hide the centre's secret; it appears to give a high collusion threshold.

023623 ‘A Simple ID-Based Scheme for Key Sharing’
S Tsujii, JH Chao, K Araki, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 730 - 734*

The authors propose a new noninteractive ID-based key sharing scheme. In previous such schemes, both centre and individual secrets had the form of vectors, between which linear relationships held, with the result that members could collude and use linear algebra to recover the centre secrets. The new scheme adds in random numbers to the individual secrets in order to prevent this.

023624 ‘A Digital Signature Public-Key System Based on Error Correcting Codes’
XM Wang, *Journal of the China Institute of Communications v 14 no 1 (Jan 1993) pp 34 - 39 (in Chinese)*

This paper presents a simple digital signature scheme based on error correcting codes. It uses on matrix factorisation, and has the advantage that it can correct errors in the received message as well as vouching for its authenticity.

023625 ‘Determination of the true value of the Euler totient function in the RSA cryptosystems from a set of possibilities’
CK Wu, XM Wang, *Electronics Letters v 29 no 1 (7 Jan 1993) pp 84 - 85*

If some implementation weakness makes it worthwhile to attack RSA by guessing $\phi(n)$, then these guesses can be checked quickly using the equation $2^{\phi(n)} \equiv 1 \pmod{n}$.

023626 ‘New digital signature scheme based on discrete logarithm’
SM Yen, CS Laih, *Electronics Letters v 29 no 12 (10 June 1993) pp 1120 - 1121*

The authors propose a variant of the Schnorr signature scheme; where the user’s secret key is x and his public key is $y = g^x$ (Mod p), and $q \mid (p-1)$, the signature of m is (r, s) where $r = g^k$ (mod p) for some random message key k, and $s = x + krm$ (mod q).

023627 ‘Immunising Public Key Cryptosystems Against Chosen Ciphertext Attacks’
YL Zheng, J Seberry, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 715 - 724*

The authors show how adaptive chosen ciphertext attacks might possibly arise in practice, and then show how either hash functions or digital signature schemes can be used to prevent them. They develop a formal structure within which security relative to such attacks can be proved.

7 Computational Number Theory

023701 'A subexponential algorithm for discrete logarithms over all finite fields'
LM Adleman, J Demarrais, *Mathematics of Computation v 61 no 203 (July 1993) pp 1 - 15*

The authors extend index calculus methods from prime fields to the arbitrary finite field $GF(q)$ where $q = p^n$. The idea here is to solve $\alpha^x = \beta$ by calculating a lot of $\gamma = \alpha^r \beta^s$, and retaining those for which γ is smooth. In $GF(q)$, this means developing suitable definitions of smoothness and other algebraic machinery; in particular, the field is represented as $\mathcal{O}/(p)$ for $n < p$, where $\mathcal{O}$ is a suitable integer ring, and as $(Z/pZ[x])/(f)$ for $n > p$. The running time is expected to be $exp(C\sqrt{\log q \log\log q})$.

023702 'Double-Precision Modular Multiplication Based on a Single-Precision Modular Multiplier and a Standard CPU'
B Arazi, *IEEE Proceedings on Selected Areas in Communications v 11 no 5 (June 1993) pp 761 - 769*

The author presents a number of algorithms to double the effective size of a modular multiplier, even where this does not provide external division services, and discusses their relative performance.

023703 'Elliptic curves and primality proving'
AOL Atkin, F Morain, *Mathematics of Computation v 61 no 203 (July 1993) pp 29 - 68*

The authors present an elliptic curve primality proving algorithm which improves on the Goldwasser-Killian method: instead of computing the number of points on each trial curve by Schoof's algorithm, they use complex multiplication to construct curves with a desired number of points. They discuss choice of coefficients, optimisation and empirical performance; primes of 400 decimal digits can be proved within a few days on a workstation.

023704 'Statistical evidence for small generating sets'
E Bach, L Huelsbergen, *Mathematics of Computation v 61 no 203 (July 1993) pp 69 - 82*

The authors conjecture that $G(n) \leq (\log 2)^{-1} \log n \, \log\log n$, where $G(n) = \min\{x : Z_n^* \text{ is generated by primes} \leq x\}$. This conjecture would follow from the prime number theorem if small primes in Z_m^* behaved randomly as far as the group structure was concerned; it would imply, independently of the extended Riemann hypothesis, that an m-bit number can be tested for primality in a deterministic way using $O(m^2)$ multiplications; and it is supported by numerical computation up to 10^9.

023705 'Explicit primality testing for $h.2^k \pm 1$'
W Bosma, *Mathematics of Computation v 61 no 203 (July 1993) pp 97 - 109*

The classical Lucas-Lehmer primality test for $2^k \pm 1$ is extended to $h.2^k \pm 1$. This extension seems to exist for all h except for $h = 4^m - 1$.

023706 'Factoring integers using SIMD sieves'
B Dixon, AK Lenstra, *Eurocrypt 93 pp M27 - M38*

The authors report implementing the quadratic sieve on a 16K MasPar SIMD (single instruction multiple data) computer. This factored the 110 digit RSA challenge in 20 cpu days, and can factor 100 digit numbers in 3 cpu days. This shows that such machines are more suited to factoring than was previously thought; a number of the optimisations which were used are discussed.

023707 'Average case error estimates for the strong probable prime test'
I Damgård, P Landrock, C Pomerance, *Mathematics of Computation v 61 no 203 (July 1993) pp 177 - 194*

The authors define $p_{k,t}$ as the proportion of k-bit odd numbers which pass t rounds of the Miller-Rabin test but are in fact composite. They show that $p_{k,1} \leq k^2 4^{2-\sqrt{k}}$ and get more complex formulae for a number of cases of $t \geq 2$; the result most relevant to cryptology is that for $3 \leq t \leq k/9$, $p_{k,t} \leq k^{3/2}2^t t^{-1/2}4^{2-\sqrt{tk}}$.

023708 'The factorisation of the ninth Fermat number'
AK Lenstra, HW Lenstra, MS Manasse, JM Pollard, *Mathematics of Computation v 61 no 203 (July 1993) pp 319 - 349*

This article explains the number field sieve in some detail, compares it with other factoring algorithms, and relates how it was used to factor the ninth Fermat number, $2^{512}+1$, into prime factors of 7, 49 and 99 digits. This project involved getting a large number of volunteers to collect the necessary relations on their workstations and email them to the authors, who then used a parallel machine to find the dependencies.

023709 'The Carmichael numbers up to 10^{15}'
RGE Pinch, *Mathematics of Computation v 61 no 203 (July 1993) pp 381 - 391*

The author reports that there are 105,212 Carmichael numbers up to 10^{15}, and presents tables showing how many of them lie in certain congruence classes, how many of a given size have a given number of prime factors, and the incidence of small prime factors. He also lists the smallest Carmichael number with each number of prime factors from 3 to 20.

023710 'Numerical computations concerning the ERH'
R Rumely, *Mathematics of Computation v 61 no 203 (July 1993) pp 415 - 440*

The author reports checking the extended Riemann hypothesis to height 10,000 for all primitive L-series with conductor $Q \leq 13$, and to height 2,500 for a number of other Q. This involved a distributed computation on PCs, which used about 25 MFlop years.

023711 'A practical analysis of the elliptic curve factoring algorithm'
RD Silverman, SS Wagstaff, *Mathematics of Computation v 61 no 203 (July 1 993) pp 445 - 462*

The authors present an analysis of the performance of the elliptic curve method, and show that the parameters should be steadily increased during use: this is because each time a curve fails to factor the target number, the estimated size of its smallest factor increases. They also present a table showing, for target numbers of different sizes, how much effort should be spent on the elliptic curve method before switching to the quadratic sieve.

023712 'How was F_6 factored?'
HC Williams, *Mathematics of Computation v 61 no 203 (July 1993) pp 463 - 474*

The author discusses manual factorisation algorithms in use in the 19th century, and reconstructs the techniques used by Landry in 1880 to factor $2^{64}+1$. Lucas had showed that any prime factor must be of the form $256h+1$, and indeed the factor found was $256.1071+1$; the search was speeded up by various tricks, and in particular by the use of exclusion moduli.

023713 'A refinement of H.C.Williams' qth root finding algorithm'
KS Williams, K Hardy, *Mathematics of Computation v 61 no 203 (July 1993) pp 475 - 483*

Where p and q are prime, $q \mid p$ and $a^{(p-1)/q} \equiv 1 \bmod p$, then the congruence $x^q \equiv a \bmod p$ has q solutions and Fermat's theorem cannot be used. An algorithm of Williams (which generalises the square root finding algorithm) takes $O(q^3 logp)$ steps; a variant is presented here which takes $O(q^4) + O(q^2 logp)$, and is thus faster for small q.

8 Theoretical Cryptology

023801 'Lower bounds for the probability of successful message deception'
LA Bassalygo, *Problems of Information Transmission v 23 no 2 (1993) (in Russian)*
The authors refine the results of Gilbert, MacWilliams and Sloane on unconditional authentication; in particular they generalise these authors' 'square root bound' from the case where all messages are equiprobable to the case where no one message has probability larger than one half.

023802 'Global, Unpredictable Bit Generation Without Broadcast'
D Beaver, N So, *Eurocrypt 93 pp W149 - W160*
A distributed coin tossing protocol is presented which requires only one message per bit per processor, and in which only the initialisation process need be interactive. It is based on the difficulty of factoring.

023803 'Secret-Key Reconciliation by Public Discussion'
G Brassard, L Salvail, *Eurocrypt 93 pp W135 - W148*
The author consider a problem which arises in quantum cryptography, namely how two parties who share a secret but noisy channel can correct the errors in this by public discussion in such a way as to leak an arbitrary small amount of information. The prove that this can be done in polynomial time and present an almost ideal protocol called Cascade.

023804 'Size of Shares and Probability of Cheating in Threshold Schemes'
M Carpentieri, A De Santis, U Vaccaro, *Eurocrypt 93 pp M96 - M103*
When a secret key is reconstructed in a k-out-of-n threshold scheme, $k-1$ shareholders can cheat by giving shares different from these obtained from the key distributor. They are successful if a wrong, but legal, key is computed. Using elementary information theory, it is proved that if the probability of successful cheating must be less or equal to ϵ, then the size of the shares must be at least the size of the secret plus $\log_2 1/\epsilon$.

023805 'Practical and Provably Secure Release of a Secret and Exchange of Signatures'
IB Damgård, *Eurocrypt 93 pp T49 - T63*
This paper presents a statistical zero-knowledge protocol for the gradual release of secrets or signatures. The release can be done one bit at a time; and it is also verifiable in the sense that the sender cannot cheat (such as by releasing garbage) unless he can factor a large number.

023806 'Peut-on se téléporter?'
H Guillemot, *Science et Vie no 910 (July 93) pp 40 - 45 (in French)*
Teleportation, in the sense of making an exact copy of a particle, had long seemed contrary to the Heisenberg uncertainty principle. Recent work by Bennett and others has shown that this is not the case; twinned pairs of photons (EPR pairs) can be used to transfer the quantum part of the information in a particle from one place to another. Teleportation does not after all appear to violate entrenched physical laws, such as by allowing matter to be duplicated, or by allowing information to be transmitted faster than light; it thus contributes to the philosophical debates at the heart of physics, as well as to quantum computation and quantum cryptography. As a teleported object cannot be copied, it would provide a completely secure means of communication.

023807 'On the Relation Between A-Codes and Codes Correcting Independent Errors'
T Johansson, G Kabatianskii, B Smeets, *Eurocrypt 93 pp M1 - M10*
The paper introduces new authentication codes, called I-equitable A-codes. A relation between these new authentication codes and codes correcting independent errors is given. It is proved for such codes that if the probability of successful impersonation (P_I) is equal to the probability of

performing a successful substitution attack (P_S), then the number of source states allowed can only grow linearly in function of the cardinality of the key space. However, if P_S exceeds P_I then the above growth is exponential.

023808 'Nonperfect Secret Sharing Schemes and Matroids'
K Kurosawa, K Okada, K Sakano, W Ogata, S Tsujii, *Eurocrypt 93 pp M104 - M120*

This paper defines a 'level d access hierarchy' such that the knowledge a set of shareholders A have about a secret key depends linearly on the level the set A has in this hierarchy. A sharing scheme with a level d access hierarchy is ideal if the size of the shares is $H(S)/d$, where $H(S)$ is the entropy of the secret key. Properties for such sharing schemes are given and a relation with matroids is shown.

023809 'Secret Key Agreement by Public Discussion from Common Information'
UM Maurer, *IEEE Transactions on Information Theory v 39 no 3 (May 1993) pp 733 - 742*

Suppose Alice and Bob wish to generate a shared secret key S from dependent random variables X and Y, while giving negligible information about S to an enemy Eve who knows a further dependent random variable Z. Previous protocols for this had assumed that Z was noisier than X and Y; the author shows that this assumption is unnecessary provided that Alice and Bob have a public channel which cannot be manipulated by Eve (although she is assumed to eavesdrop on it). This public channel is used to identify bits shared between Alice and Bob using a divide-and-conquer protocol; given enough of these, a key can be derived which Eve does not know.

023810 'Optimal Authentication Systems'
R Safavi-Naini, L Tombak, *Eurocrypt 93 pp M11 - M21*

Optimal authentication codes are defined as those for which, firstly, the probability of deception is $|S|/|M|$, where $|S|$ and $|M|$ are the cardinality of the source space and cryptogram space respectively; secondly, Simmons' bound on impersonation is satisfied; and thirdly Pei's bound on substitution is satisfied too. Properties of such codes are proved, and it is shown that doubly perfect systems are optimal. Construction methods for optimal codes are given.

023811 'How to Stop a Cheater: Secret Sharing with Dishonest Participation'
EW Selberg, *Carnegie Mellon Technical Report CMU-CS-93-182*

The author proposes that secret sharing schemes should have the properties that no party should be able to extract someone else's secret without revealing his own; that cheaters should be detected; and that new shares can be created to supplement or replace existing ones. A bit by bit variant of the Ben Or/Rabin scheme is presented which achieves these goals.

023812 'Universal Redundancy Rates Do Not Exist'
PC Shields, *IEEE Transactions in Information Theory v 39 no 2 (March 1993) pp 520 - 524*

Rates of convergence for redundancy are possible only for special classes of source, such as memoryless sources, Markov sources of a given order, and finite state sources with a given number of states. A counterexample is constructed to show that there is no universal redundancy rate for any sequence of prefix codes on the class of all ergodic sources.