.

Volume 6 Number 1 (March 1997) ISSN 1352-6278

CONTENTS

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

'Computer and Communications Security Reviews' is published quarterly by, and is copyright, of Northgate Consultants Ltd. Subscription rates, conditions and ordering details are on the inside back cover; note that the address for subscriptions has changed.

Editorial

In this issue, we have articles from journals received at the Cambridge University Library and Scientific Periodicals Library by March 1997, and most books and technical reports received by the editor prior to this date. We also have reviews of papers presented at the following conferences:

Protocols 96: Security Protocols – International Workshop, Cambridge, United Kingdom, April 1996; *proceedings published by Springer-Verlag as LNCS v 1189, ISBN 3-540-62494-5*

ACISP 96: Information Security and Privacy: First Australasian Conference; June 24-26, 1996, Wollongong, NSW, Australia; *proceedings published by Springer-Verlag as LNCS v 1172, ISBN 3-540-61991-7*

Database 96: Database Security Volume X: Status and prospects; July 22-24 1996, Como, Italy; IFIP TC11/WG11.3 10th International Conference on Database Security; *proceedings published by Chapman & Hall, ISBN 0-412-80820-X*

ISSAC 96: International Symposium on Symbolic and Algebraic Computation, 24–26 July 1996, Zürich, Switzerland; *proceedings published by the ACM as ISBN 0-89791-796-0*

Cardis 96: Smart card Research and Advanced Applications, 2nd International Conference; September 16-18, 1996, CWI, Amsterdam, The Netherlands; *proceedings published by Stichting Mathematisch Centrum, ISBN 90-6196-465-2*

ESORICS 96: Fourth European Symposium on Research in Computer Security, 25–27 September 1996, Rome, Italy; *proceedings published by Springer as LNCS v 1146*

LISA 96: Tenth Large Information Systems Administration Conference, 29 September – 4 October 1996, Chicago, Illinois; *proceedings published by the Usenix Association, ISBN 1-880446-81-1*

Asiacrypt 96: International Conference on the Theory and Applications of Cryptology and Information Security, Kyongju, Korea, 3–7 November 1996; *proceedings published by Springer-Verlag as LNCS v 1163, ISBN 3-540-61872-4*

Multimedia 96: Fourth ACM International Multimedia Conference, 18–22 November 1996, Boston, Massachussetts; *proceedings published by the ACM as ISBN 0-89791-871-1*

Apps 96: 12th Annual Computer Security Applications Conference, San Diego CA, December 9-13 1996; *proceedings published by the IEEE, ISBN 0-8186-7606-X*; some of these were reviewed in v 5 no 4

RSA 97: 1997 RSA Data Security Conference, 28–31 January 1997, San Francisco, California; *proceedings published by RSA DSI Inc.*

We place an electronic version of this journal in the public domain one year after publication. The goal is to strike a balance between providing a universal service and maintaining enough revenue to cover the costs of publication. Subscribers get paper copies and up-to-date electronic versions as well; subscription information may be found inside the back cover. The archives can be found at `http://www.cl.cam.ac.uk/users/rja14/#SR`.

1 Applications and Engineering

061101 'Biometrics on Smartcards: An Approach to Keyboard Behavioral Signature'
TJ Alexandre, *Cardis 96 pp 25–37*

A new keyboard typing biometric is introduced. The frequencies of single and paired characters are measured when users press eight keys with both hands. The algorithm is aimed at a smartcard application, and a neural network implementation is also discussed.

061102 'Signature verification using multiple neural classifiers'
R Bajaj, S Chaudhury, *Pattern Recognition v 30 no 1 (97) pp 1–7*

The authors describe using a feedforward neural net to classify signatures based on projection movements and the upper and lower envelope characteristics; the output of the three classifiers is combined using a connectionist scheme. When trained using five genuine signatures from each of ten individuals, it was set to classify ten genuine signatures from each of them and a hundred random forgeries. While the individual classifiers' false accept rates were in the range 8–12%, combining them gave 6.5% and learning reduced it further to 3%.

061103 'Nasdaq's technology floor: its president takes stock'
AR Berkeley, *IEEE Spectrum v 34 no 2 (Feb 97) pp 66–67*

Nasdaq's president describes the company's systems, including an intrusion detection system called SWAT (Stock Watch Automated Tracking) that looks for discrepancies in trading patterns that could indicate insider dealing.

061104 'Datenschutzorientierte Abrechnung medizinischer Leistungen'
G Bleumer, M Schunter, *Datenschutz und Datensicherheit v 21 no 2 (Feb 97) pp 88–97*

The authors discuss how de-identification mechanisms can be used to protect medical privacy, and outline a design for a cryptographic credential system that enables healthcare providers such as state bodies or insurance companies settle bills, control costs and maintain auditability and accountability, without revealing the binding between individual medical records and patients' identities.

061105 'Challenges for copyright in a digital age'
ID Bramhill, MRC Sims, *BT Technology Journal v 15 no 2 (Apr 97) pp 63–73*

The authors talk about copyright management technology, including DVD and watermarking; he suggests binding licensed content to machine characteristics such as hardware configuration, bad disk sectors and the file system structure.

061106 'Firewall Protection Without the Pitfalls'
L Bruno, *Data Communications International (Mar 97) pp 31–32*

This article describes an NT-based proxy firewall product designed to integrate with NT domains and to be particularly simple to configure.

061107 'Smart card use to manage user's mobility'
D Carlier, S Lecomte, P Trane, *Cardis 96 pp 157–174*

A system for mobile utilisation of computer resources through agent technology is discussed. Smartcards are used to ensure security, principally through authentication.

061108 ' "Minting" electronic cash'
D Chaum, S Brands, *IEEE Spectrum v 34 no 2 (Feb 97) pp 30–34*

The authors describe some electronic cash systems and discuss some of the options and tradeoffs available when engineering such systems.

061109 'Securing the Residential Asynchronous Transfer Mode Networks'
SC Chuang, D Greaves, *Protocols 96 pp 177–196*

This paper analyses security management within a residential ATM network — the ATM Warren — in which an ATM fabric pervades the home and connects many appliances that are currently dumb or furnished with their own microcontroller. It points out some threats, and discusses the applicability of cryptographic devices for firewall and other protection in the context of a user who controls his home with an infra-red remote control. It presents a data path protection mechanism that can guard against masquerading, eavesdropping and message modification attacks.

061110 'Heavy-Duty Security at Half Price'
A Cray, *Data Communications International (Jan 97) pp 87–88*

This article describes a low cost encryption software toolkit that can provide IP layer encryption using SSH.

061111 'Router Encryption Made Easy — The Hard Way'
A Cray, *Data Communications International (Feb 97) pp 36–38*

This article describes an IP encryption product — a hardware add-on for routers that can encrypt traffic with little CPU overhead.

061112 'Intelligent Security Reporting: Auditing Security Logs'
N Crocker, *Computer Audit Update (Feb 97) pp 8–17*

The author describes some simple screening systems: one calls attention to accounts on which three or more failed login attempts have been made in 24 hours, while another emails users' managers whenever they try to access a prohibited resource. He stresses the need for such intrusion detection systems to be evaluated: are they detecting anything? Are they missing anything?

061113 'Fast forward on the hi-tech highway'
C Davis, *Cards International no 173 (28/2/97) pp 12–15*

This survey of online retail payment mechanisms in the USA combines synopses of a number of market surveys and predictions, reviews of AI techniques in data mining and the development of SET, and a look at a smartcard reader that fits in a PC.

061114 'Lossless Compression Algorithms for Smart Cards: A Progress Report'
JF Dhem, JJ Quisquater, R Lecat, *Cardis 96 pp 73–88*

Ways to select data compression approaches for the smartcard implementations are discussed. Huffman and arithmetic compression are found to be most suitable for the current cards. Some comparative evaluations are provided, and adaptations of the algorithms are discussed.

061115 'Pointing the finger'
I Drury, *Security Surveyor v 27 no 5 (Jan 97) pp 15–17*

This article describes a fingerprint recognition system for building access control that is already used in Frankfurt and Vienna airports, as well as in nuclear power stations in Switzerland and Germany.

061116 'Electronic commerce comes to the web'
JA Edelheit, MR Miller, *BT Technology Journal v 15 no 2 (Apr 97) pp 24–31*

This is a phone company view of the history of electronic commerce; it has a strong focus on EDI.

061117 'Case-Based Reasoning for Intrusion Detection'
M Esmaili, R Safavi-Naini, B Balachandran, J Pieprzyk, *Apps 96 pp 214–223*

A case-based reasoning for intrusion detection is presented. Low level audit records, such as lists of Unix commands, are translated into a high level class representation,

which is then input to a detection system. The degree of risk detected is represented by a probability.

061118 'Evidential Reasoning in Network Intrusion Detection Systems'
M Esmaili, R Safavi-Naini, J Pieprzyk, *ACISP 96 pp 253–265*

A model for intrusion detection systems is presented, based on gathering evidence on user behaviour, followed by evidential reasoning to deal with uncertainty in an expert system. However, it requires a good model of intrusive behaviour, and rules for the expert system.

061119 'Cowry shell to smart card'
D Everett, *IEE Review v 43 no 2 (20/3/97) pp 59–62*

A Mondex developer talks about the project's progress to date.

061120 'FAME: A 3rd Generation Coprocessor for Optimising Public Key Cryptosystems in Smart Card Applications'
R Ferreira, R Malzahn, P Marissen, JJ Quisquater, T Wille, *Cardis 96 pp 59–72*

The authors present a new architecture for implementing public key cryptosystems in smartcards, based on a coprocessor, and give performance figures.

061121 'In your pocket: smartcards'
CH Fancher, *IEEE Spectrum v 34 no 2 (Feb 97) pp 47–53*

This article talks about smartcards, their standards and some applications.

061122 'Off-the-shelf, on to sea'
D Foxwell, *International Defense Review v 30 (Jan 97) pp 33–38*

This article describes a number of naval command and control systems being developed (or already fielded) in the UK, France, Sweden and elsewhere. These show a strong preference for standards such as Posix, X and (increasingly) Windows. It discusses how systems can be hardened for shock and radiation, and the management of hardware redundancy: several manufacturers implement a 'virtual machine' on top of multiple servers. The main problem is configuration control, as commercial products continue to evolve. Other problems include poor support for Ada, for realtime operations and for MLS integration.

061123 'Data privacy in medicine: a perspective offered by the Data Protection Registrar'
E France, *British Journal of Healthcare Computing and Information Management v 14 no 2 (Mar 97) pp 20–22*

Britain's Data Protection Registrar examines some of the privacy problems of recently introduced healthcare systems and calls for the greater use of privacy enhancing technologies such as the de-identification of personal data.

061124 'Banks fingerprint customers to cut cheque fraud'
Fraud Watch Q1 97 p 9

Many US banks are starting to fingerprint customers who open new accounts, and non-customers who cash cheques; they claim that it cuts fraud by about half, and that there is little customer resistance when scanners (as opposed to ink and paper) are used. MasterCard is planning to roll out smartcard based fingerprint scanning worldwide if pilots succeed; it plans to look for opportunities to market its system for ID cards, welfare benefits cards, passports and so on. However, there is a proposal in the Georgia legislature to make it illegal for banks to demand fingerprints.

061125 'EP schemes — secure but not invincible'
Fraud Watch Q1 97 pp 1–2

This article contains statements from a number of vendors about electronic purse security; their common theme is that the technical protection is adequate for prepaid cards with limits of \$50 – \$100.

061126 'SET to beat the fraudsters?'
Fraud Watch Q1 97 pp 4–5

This article relates the view of a senior MasterCard VP that SET will ultimately be hacked, but that it is part of the learning process.

061127 'BT HealthNet — an early intranet case study'
AJ Frost, *BT Technology Journal v 15 no 2 (Apr 97) pp 114–125*

This article describes an intranet constructed for Britain's National Health Service, with particular emphasis on its firewall-based security mechanisms.

061128 'Has Cash Had its Chips?'
E Hallatt, *Security Surveyer v 27 no 5 (Jan 97) pp 10–13*

This article talks about a number of electronic purse trials.

061129 'Enigma: actions involved in the "double stepping" of the middle rotor

DH Hamer, *Cryptologia v XXI no 1 (Jan 97) pp 47–50*

The author describes the internal machine actions involved in the double stepping of the Enigma's middle rotor.

061130 'The Design and Implementation of a Network Account Management System'
JA Harris, *LISA 96 pp 33–41*

The author describes a tool, NAMS, developed at James Madison University to do remote Unix system administration. An interesting security problems arose in the context of managing password 'clusters': users were initially allowed to define more than one group of accounts, so that they could, for example, use different passwords for accounts at different sensitivity levels. However, it was so difficult to stop attacks based on redefining clusters that the final system limits the ability to change clusters to the system administrator.

061131 'The importance of moral and legal regulation of the EPR'
S Heard, L Doyal, *British Journal of Healthcare Computing and Information Management v 14 no 2 (Mar 97) pp 26–28*

The authors discuss what measures are likely to be necessary to protect electronic patient records if these become an integrated and universal means of recording personal health information. They describe a number of relevant legal principles, and the likely effects of the EU directive.

061132 'Priv: Secure and Flexible Privileged Access Dissemination'
BC Hill, *LISA 96 pp 1–8*

The author discusses the pros and cons of a number of tools that allow users controlled access to privileged Unix commands, and describes Priv — a tool that enables such controlled access to be granted in a consistent way. Commands may be restricted by user, host or operating system type, in an inclusive or exclusive way; templates can be used to constrain parameters; and use can be logged with a level of detail tailored to the command.

061133 'Protection of Software Algorithms Executed on Secure Microprocessors'
HDL Hollmann, JPMG Linnartz, JH van Lint, CPMJ Baggen, LMG Tolhuizen, *Cardis 96 pp 133–143*

The problem of executing an algorithm without revealing the instructions or parameters to external observers is discussed. Dummy instructions can be loaded; ways of distinguishing these from real instructions are discussed, leading to a conclusion that dummy reads should not be chosen at random in certain cases.

061134 'Security Measures for the Austrian "PAYCHIP" Electronic Purse Application'
M Holzbach, *Apps 96 pp 69–77*

The author provides an overview of the developments within Austria's 'Paychip' smartcard electronic purse system. This has been led by commercial banks, monitored by the National Bank, and involved evaluations from the German BSI and Dutch TNO. The security policy for the entire system was developed, as well as a new ITSEC functionality class F-ZS. The maximum amount loaded into a purse is about $190; encryption is done with single and triple DES.

061135 'Single Sign-On and Security — An Overview'
M Horrell, *Information Security Bulletin v 2 no 1 (Jan 97) pp 39–49*

This article looks at a number of different approaches to single sign-on, and lists a number of products.

061136 'Off-line signature verification based on geometric feature extraction and neural network classification'
K Huang, H Yan, *Pattern Recognition v 30 no 1 (97) pp 9–17*

The authors describe a system to identify images of signatures by examining the image's geometric features at several scales simultaneously using several different neural network classifiers. This achieved 90% correct classification against a database of 3,000 images.

061137 'Firewalling the Net'
SD Hubbard, JC Sayer, *BT Technology Journal v 15 no 2 (Apr 97) pp 94–106*

This article reviews firewall technology, and briefly describes implementing a firewall system for a corporate client.

061138 'A Comparison of the Iridium and AMPS Systems'
YC Hubbel, *IEEE Network v 11 no 2 (Mar/Apr 97) pp 52–59*

The protocols to be used in Iridium are described. Although users will be issued with smartcards, the underlying protocols appear much more similar to the US AMPS system than to GSM.

061139 'UK Royal Navy digests FOCSLE experience'
International Defense Review v 30 (Mar 97) p 18

This article describes an MLS system developed for the Royal Navy headquarters at Northwood, and now installed there and at a number of remote sites. Using Alpha hardware, it combines a database from Jane's, input on shipping movements from Lloyd's, and classified intelligence inputs. It is claimed to be one of the first MLS systems based on commercial off-the-shelf equipment to enter service.

061140 'Checking on-line'
MA Johnson, H Baulch, *IEEE Spectrum v 34 no 2 (Feb 97) pp 58–59*

This article describes the systems used by CheckFree, a US service provider that processes payment instructions generated by bank customers using their PCs.

061141 'Model for network behaviour under viral attack'
S Katsikas, T Spyrou, D Gritzalis, J Darzentas, *Computer Communications v 19 (96) pp 124–132*

The authors model viral intrusions by considering network nodes to have four states — disabled, normal, infected (and infectious), and antidotal (able to detect infection at other nodes, and to cure infected nodes. Simulation results are given for the state transitions induced by this model; the idea is to enable administrators work out how many nodes to protect to what level.

061142 'Limiting the Visible Space Visual Secret Sharing Schemes and Their Application to Human Identification'
K Kobara, H Imai, *Asiacrypt 96 pp 185–195*

The paper elaborates on the use of visual secret sharing scheme of Naor and Shamir from **032134** to limit the volume of space from which a decoded image can be seen. The visibility of the image from various viewpoints is discussed, and an application to human identification is given.

061143 'Smart Cards — Is Britain Smart Enough?'
A Laird, *Computer Fraud and Security Bulletin (Feb 97) pp 11–15*

A smartcard company manager describes some systems fielded in the UK, which he claims is five years behind Europe in applying this technology.

061144 'Direct Gray-Scale Minutiae Detection in Fingerprints'
D Maio, D Maltoni, *IEEE Transactions on Pattern Analysis and Machine Intelligence v 19 no 1 (Jan 97) pp 27–40*

The authors survey existing techniques for identifying fingerprints; most of them work by matching minutiae and are hard to do with low-quality images. They describe a preprocessing algorithm, called ridge line following, that enables many of the false minutiae (such as breaks in ridge lines arising from noise artifacts) to be removed.

061145 'Secure Concurrency Control in MLS Databases with Two Versions of Data'
LV Mancini, I Ray, *ESORICS 96 pp 304–323*

The authors propose a secure lock based concurrency protocol for multilevel secure databases. The protocol uses two versions of the data: one a committed version on which all the read operations are performed (regardless of level), and an uncommitted version on which all the write operations are performed.

061146 'Enhancing the Controlled Disclosure of Sensitive Information'
DG Marks, A Motro, S Jajodia *ESORICS 96 pp 290–303*

In **034218**, the authors presented a method for preventing the aggregation of information disclosures made by a database using query sequence control: data that had already been disclosed to each user are stored as subviews. In order to prevent attacks involving combinations of queries, they extend this work by protecting the key projections of a sensitive concept.

061147 'Banking in cyberspace: an investment in itself'
MC McChesney, *IEEE Spectrum v 34 no 2 (Feb 97) pp 54–59*

Some of the protection mechanisms used by Security First Network Bank are described. They are based on using an MLS system to protect internal applications from network attacks.

061148 'Centralised Administration of Distributed Firewalls'
M Miller, J Morris, *LISA 96 pp 19–23*

The authors describe a system built by Bell Atlantic for centralised security administration. They standardised on Sun for the firewalls and Cisco for the routers, but nonetheless have a variety of configurations; public domain software is used, including Tripwire to detect changes to security critical files and Tiger to do regular audits, while a home-grown intrusion detection system parses and filters error messages.

061149 'Arithmetic co-processors for public-key cryptography: The State of the Art'
D Naccache, D M'Raïhi, *Cardis 96 pp 39–58*

The paper reviews current smartcard technology, and provides a comparative review of marketed products with particular reference to manufacturers' algorithms for doing modular multiplication. There is also a perspective on PCMCIA, and smartcard technology purchasing suggestions.

061150 'Computer Virus-Antivirus Coevolution'
C Nachenberg, *Communications of the ACM v 40 no 1 (Jan 97) pp 46–51*

This article traces the history of how antivirus programs influenced virus design, and vice versa. It also describes the new 'generic decryption' technique used to find polymorphic viruses: the code under test is run in a software emulation of the CPU and watched to see if it decrypts a recognisable virus body.

061151 'Automatic On-Line Signature Verification'
VS Nalwa, *Proceedings of the IEEE v 85 no 2 (Feb 97) pp 215–239*

The author proposes an algorithm for identifying signatures on-line based on an elastic local-shape-based model. Each curve is parametrised and measures analogous to centre of mass, torque and moment of inertia are computed. Means of dealing with variation are discussed, together with the results of lab tests. The claimed advantage over other systems is the ability to cope with signers who sometimes sign ballistically and at other times sign deliberately.

061152 'Health information privacy and confidentiality: a case study of the Antipodes'
R Neame, *British Journal of Healthcare Computing and Information Management v 14 no 2 (Mar 97) pp 29–32, 42*

This article describes how the privacy of electronic medical records is managed in New Zealand. The main protection mechanism is that centrally archived medical records, which are used for research and planning purposes, have had identifiers encrypted; the secondary mechanism is that any enquiry that would be answered with reference to fewer than six records is blocked. By contrast, Australia has some standards documents, but little fielded protection.

061153 'Firewalls: don't get burned'
D Newman, H Holzbauer, K Bishop, *Data Communications International (21/3/97) pp 36–53*

In a lengthy survey, the firewall offerings from nineteen vendors are put through their paces and evaluated for security, manageability and performance. Almost 100 different kinds of attack were tried; most products did fairly well against most penetration tests, but many lacked some important features (such as screening out ActiveX and other mobile code), while many performed badly or not at all under high traffic volumes. In fact, only five could cope with 50 Mbit/sec traffic.

061154 'Dual eigenspace method for human face recognition'
H Peng, D Zhang, *Electronics Letters v 33 no 4 (13/2/97) pp 283–284*

The main obstacle to reliable human face recognition is locating facial features, especially when head posture, lighting conditions and facial expressions vary. Eigenface techniques in particular suffer from the problem that some eigenvectors capture 'noise' due to illumination and expression. The proposed fix is to have a separate set of eigenvectors for each person, and empirical results suggest that with 8 or more training samples per person, one can get a recognition rate of 97–98% as opposed to the 92–93% given by traditional methods.

061155 'Pseudonyms for Cancer Registries'
K Pommerening, M Miller, I Schmidtmann, J Michaelis, *Methods of Information in Medicine v 35 (96) pp 112–121*

The authors describe a system now fielded in Germany whereby de-identified records of patients with cancer are collected into a central state registry to support research. A trusted office is responsible for pseudonym allocation and record deduplication; record linkage is cryptographically controlled. Other security concerns and measures are described too. Initial experience in Rheinland-Pfalz indicates that the concept is sound, and it is being adopted in other German states.

061156 'Electronic Payment Systems'
P Putland, J Hill, D Tsapakidis, *BT Technology Journal v 15 no 2 (Apr 97) pp 32–38*

This article talks about various transaction models in electronic commerce, and describes a micropayment scheme being introduced by BT.

061157 'Confidentiality — fact or fiction? A consumer's view of when faith is broken'
J Robinson, *British Journal of Healthcare Computing and Information Management v 14 no 2 (Mar 97) pp 24–25*

The author describes a number of failures of medical confidentiality, and of conflicts with research and other professional interests in which the patient usually comes off worst.

061158 'When Firewalls Fail: Lessons Learned from Firewall Testing'
EE Schultz, *Network Security (Feb 97) pp 8–11*

Firewall testing conducted by SRI has shown that the most frequent vulnerabilities are those in unscreened hosts protected by the firewall, followed by services on the firewall itself, and interactions between the firewall and the external router or a host on the DMZ (see **052138**). Most firewalls are fairly vulnerable to attack from the router and host inside the DMZ, but resist attacks from completely unknown external IP addresses.

061159 'Encryption'
Secure Computing (Feb 97) pp 45–58

This article reviews and compares fourteen PC file encryption products.

061160 'Shuse: Multi-Host Account Administration'
H Spencer, *LISA 96 pp 25–32*

The author describes a system developed for a university in Ontario that manages accounts centrally for a diverse population of Unix systems.

061161 'A Comparative Study of Electronic Purses'
Supplement to Smart Card News v 6 no 2 (Feb 97)

This booklet tabulates details of 34 electronic purse schemes being planned or tried out in a number of countries, and provides sketchier details on some others.

061162 'Methods for Encrypting and Decrypting MPEG Video Data Efficiently'
L Tang, *Multimedia 96 pp 219–229*

The author looks at ways to combine encryption with MPEG compression. Previous proposals to encrypt only I-frames had been shown to be insecure by Agi and Gong in **053102**; the fix presented here is to also scramble the zig-zag order in which the picture blocks are processed. Six different ways of doing this are discussed, and their relative security analysed.

061163 'UNIX Host Administration in a Heterogeneous Distributed Computing Environment'
GS Thomas, JO Schroeder, ME Orcutt, DC Johnson, JT Simmelink, JP Moore, *LISA 96 pp 43–50*

The authors describe software they wrote for the US Pacific Northwest National Laboratory to centralise Unix administration and let users find out information such as which machines they have accounts on.

061164 'PC Administration Tools: Using Linux to Manage Personal Computers'
J Trocki, *LISA 96 pp 187–192*

The author describes PCADM, a toolkit for remote administration of PCs running the Linux operating system. It is useful even when the PCs run DOS or Windows

most of the time, allowing remote upgrades and so on to be controlled better than with existing Windows tools.

061165 'Electronic Money and Key Management from Global and Regional Points of View'
S Tsujii, *Asiacrypt 96 pp 173–184*

This invited talk reviews issues of electronic commerce with respect to cultural and political concepts — mainly problems with electronic money and cryptography policy.

061166 'Web servers tuned for e-commerce'
MJ Tucker, *Datamation (Feb 97) pp 92–98*

The author discusses factors to be considered when buying a commerce server; a frequently overlooked requirement is support for EDI and for legacy banking systems. He also describes some problems with Microsoft's Merchant Server product, and mentions the overhead that SSL encryption can impose.

061167 'Development of a Secure Electronic Marketplace for Europe'
M Waidner, *ESORICS 96 pp 1–14*

This article provides an overview of the EU project SEMPER (Secure Electronic Marketplace for Europe) whose goals are to develop, implement and test an open and system independent architecture for electronic commerce.

061168 'The Impact of Multilevel Security on Database Buffer Management'
A Warner, Q Li, T Keefe, S Pal, *ESORICS 96 pp 266–289*

This article analyses security requirements on buffer management for multilevel secure DBMSs. It presents solutions for page allocation, replacement and read/write conflict resolution. A performance analysis of a simulation for some of these problems is given.

061169 'Software Security and the DirectPlay API'
A Wilson, *Dr Dobbs' Journal (Apr 97) pp 66–70*

Once computers are networked, detecting software piracy may become easier: programs can look for a licence server and for other instances of themselves. Some of the ramifications of this are discussed, together with ways of implementing such a system to control the number of users of a network game that uses Microsoft's DirectPlay API. Techniques are discussed for defeating standard attacks using tools such as SoftIce.

061170 'A Digital Watermarking System for Multimedia Copyright Protection'
J Zhao, E Koch, *Multimedia 96 pp 443–444*

The authors describe the main features of SysCoP, a digital watermarking system developed by the Fraunhofer Institute in Darmstadt. Label codes are embedded at locations determined with reference to extracted (geometric) features as well as a pseudorandom sequence generator.

061171 'Look, It's Not There'
J Zhao, *Byte (Jan 97) pp 401–407*

This general introduction to watermarking techniques discusses the general protection goals of this technology and the ideas underlying a number of implementations, particularly spread-sequence, frequency hopping and transform techniques.

2 Operating System and Database Security

061201 'An information theoretic analysis of architectures for multilevel secure databases'
JE Aisbett, *Database 96 pp 212–225*

The author analyses the value of information in a relational database, and of providing security in a generic multilevel secure database. He estimates parameters and values, given certain assumptions. Data classification, database usage and access control are considered in his analysis.

061202 'The expressive power of multi-parent creation in monotonic access control models'
P Ammann, RS Sandhu, R Lipton, *Journal of Computer Security v 4 no 2/3 (Dec 96) pp 149–165*

This paper shows that single-parent creation is strictly less expressive than multi-parent creation in monotonic access control models provided that subjects and objects are not destroyed and no access rights are deleted. Multi-parent creation operations can implement solutions to mutual suspicion problems, confinement, originator control, and separation of duties; this paper furnishes grounds for regarding it as a fundamental primitive operation.

061203 'An Authorisation Model for Workflows'
V Atluri, WK Huang, *ESORICS 96 pp 44–64*

The article proposes an authorisation model for workflow that is capable of synchronising the authorisation flow along with the workflow. The model presents features to deal with roles and relaxation of duties too.

061204 'An Extended Petri Net Model for Supporting Workflows in a Multilevel Secure Environment'
V Atluri, WK Huang, *Database 96 pp 240–258*

Petri nets are used to model control flow dependencies; conflicts of task dependencies in a workflow with multilevel security constraints are identified. A 'secure Petri nets model' is given that incorporates multilevel secure constraints, as well as algorithms to construct and execute multilevel secure transactions.

061205 'Multilevel Secure Transaction Processing: Status and Prospects'
V Atluri, S Jajodia, TF Keefe, C McCollum, R Mukkamala, *Database 96 pp 79–98*

This panel discussion paper reviews the problem of transaction processing, its conventional solution, and how it conflicts with multilevel security constraints. Solutions implemented by commercial vendors, as well as some emerging ones, are described. The authors explain the challenges in algorithms for advanced transaction models, index and recovery methods, buffer management, transaction processing performance and data repair.

061206 'Modeling A Multi-level Secure Object-Oriented Database Using Views'
A Baraani-Dastjerdi, J Pieprzyk, R Safavi-Naini, *ACISP 96 pp 190–206*

The paper describes a way to derive a multi-level view model from a single-level secure object-oriented database. Operations on multi-level views are decomposed into operations on single-level objects, implementable with any conventional mandatory security kernel. Views and multi-level views can be constructed via top-down (specialisation) or bottom-up (generalisation) approach. The multi-level security properties of this model are described.

061207 'Formal Techniques for an ITSEC-E4 Secure Gateway'
P Bieber, *Apps 96 pp 236–245*

The process of defining a multi-level security policy for a secure gateway is described, followed by a presentation of deriving the formal model based on Bell-LaPadula and finally the interpretation of the formal security model is explained. All these steps are presented as part of the work on the product's ITSEC E4 evaluation.

061208 'How Smart Cards Can Take Benefits from Object-Oriented Technologies'
P Biget, P George, JJ Vandewalle, *Cardis 96 pp 175–194*

The authors argue for the next generation of smartcard operating systems to use object-oriented technology; they discuss the basic principles of this and describe a card interface to CORBA.

061209 'Merging Heterogeneous Security Orderings'
PA Bonatti, ML Sapino, VS Subrahmanian, *ESORICS 96 pp 183–197*

The authors present a technique to merge multiple security orderings into a single unified ordering that preserves the security relationships between orderings. The technique uses logic programming and graph theory.

061210 'A Comparison of Multilevel Structured Query Language (SQL) Implementations'
RK Burns, YF Koh, *Apps 96 pp 192–202*

The authors provide a comparison of SQL extensions for Informix Online/Secure, Trusted Oracle, Trusted Rubix and Sybase Secure SQL Server. Also, recommendations for a multi-level SQL standard are provided; these could enable interoperability among multi-level DBMS and standard client applications.

061211 'An Approach To Deriving Global Authorizations in Federated Database Systems'
S Castano, *Database 96 pp 58–75*

A semi-automatic approach to deriving global authorisations is presented. Firstly, local authorisations are analysed, then subject profiles are defined and used for authorisation comparison. Secondly, these subject profiles are classified. Thirdly, local authorisations are abstracted by pairs in a given cluster to global authorisation and global roles are defined. The basic global authorisations can be then manually refined.

061212 'A secure World-Wide-Web daemon'
FB Cohen, *Computers and Security v 15 no 8 (1996) pp 707–724*

The author describes a number of vulnerabilities recently found in WWW server implementations, and points out that httpd's 8000 lines of code is a huge amount for a file copying utility; it also duplicates ad-hoc many functions already found in the underlying operating system, such as directory and file access control. He sets out design criteria for secure daemons, and presents such a daemon for http — with fully described source code. Despite having strictly limited function and running as user code, it still supports over 99% of WWW services (an exception is 'post'). It has fixed buffers, output file confinement, finite runtime and multiple protection mechanisms. He also provides source code for a similar secure gopher server.

061213 'A Logical Approach to Model a Multilevel Object Oriented Database'
F Cuppens, A Gabillon, *Database 96 pp 145–166*

A semantics based on first-order logic is used to represent object-oriented database content. It lets designers formalise aspects of multilevel security, with particular detail given to formalising polyinstantiation prevention. The formalism is implemented in a model described in **031207**.

061214 'An Authorization Model for Federated Systems'
S De Capitani di Vimercati, P Samarati, *ESORICS 96 pp 99–117*

The authors present an authorisation model suitable for a tightly coupled federated system. It allows users to specify the specific access modes and the administrative policy establishing how authorisations on objects are to be defined. An algorithm describing the controls to be enforced under different authentication and administrative options is also presented.

061215 'Extensible and Reusable Role-Based Object-Oriented Security'
SA Demurjian, TC Ting, M Price, MY Hu, *Database 96 pp 288–307*

The paper investigates the application of user-role based security to object-oriented systems. Exception handling capabilities are identified as a useful way of encapsulating and hiding security details from software engineers. Generic security classes are considered vital to object-oriented systems security.

061216 'A Role-Based Secure Database Design Tool'
L Giuri, P Iglio, *Apps 96 pp 203–212*

A tool for conceptual database design and analysis is presented. The tool should assist in the discovery of potential security design flaws; it also translates the conceptual secure data scheme into the SQL specification. Role-based access control is supported.

061217 'Safe Internet Surfing'
D Greenfield, *Data Communications International (Jan 97) pp 90–92*

This article describes a firewall that examines the code of Java applets and filters out those that appear to contravene a system security policy.

061218 'A Data Model for a Multilevel Replicated X.500 Server'
G Grossman, M Schaefer, *Database 96 pp 195–211*

A model for a multilevel X.500 directory is provided, implementing storage of directory entries in a polyinstantiated multilevel tree and defining semantics of update operations that protect the tree's integrity. The model has initial and secure states defined.

061219 'On the Modelling of Preventive Security Based on a PC Network Intrusion Experiment'
U Gustafson, E Jonsson, T Olovsson, *ACISP 96 pp 242–252*

A realistic university intrusion experiment with a Novell NetWare 3.12 and last-year undergraduates is described. A compilation of the data and first-hand interpretation are provided. This is used to discuss the quantitative modelling of preventive security.

061220 'A Framework for High Assurance Security of Distributed Objects'
J Hale, J Threet, S Shenoi, *Database 96 pp 101–119*

The authors introduce a layered architecture for developing heterogeneous distributed object systems with high assurance. The four layers start from a layer of process calculus for modelling distributed object systems; a HOL semantics for each successive layer is basis of the verification framework. Constructions of upper layers might get to architectures like CORBA or DCE.

061221 'A Framework for Inference-Directed Data Mining'
TH Hinke, HS Delugach, R Wolf, *Database 96 pp 229–239*

The authors discuss how to detect inferences without either functional dependencies or foreign keys. They analyse cases where a small number of values in the target entity that can be associated with a single value in an 'anchor' entity. A data sieve approach can be used to examine a data model to detect such cases. However, data mining can still be used where a vulnerability is not detected at the model level.

061222 'Secure Locking Protocols for Multilevel Database Management Systems'
S Jajodia, LV Mancini, I Ray, *Database 96 pp 177–194*

Two algorithms for lock-based concurrency control of multilevel transactions are described. Both are based on colouring transactions and data items to prevent cycles. Only the lock manager is required to be trusted and should be easily verifiable consisting only of about a thousand lines of code. Both algorithms avoid aborting high transactions when only some of their low locks are broken, and both maintain single version data.

061223 'On the Quantitative Assessment of Behavioural Security'
E Jonsson, M Andersson, *ACISP 96 pp 228–241*

The behavioural security characteristics of a system are defined as its availability and confidentiality, whereas integrity is regarded as a preventive characteristic. A way to measure behavioural characteristics is defined, based on a user-defined set of services and their failure rates which quantify the degradation at different levels. An example with a reference monitor is given.

061224 'An Extended Capability Architecture to Enforce Dynamic Access Control Policies'
IL Kao, R Chow, *Apps 96 pp 148–157*

The concept of extended capability from **054227** is introduced. An extended capability consists of user identity and type, rights, expiration time, access control policy number and policy dependent information, and a check-field. The presented system should effectively enforce dynamic access policies. Some of the issues and applications for several security policies are discussed.

061225 'Using a Proxy X Server To Facilitate COTS Application Integration'
EM Kayden, *Apps 96 pp 185–190*

The interaction of a trusted X Window server and some COTS applications causes problems when the X clients attempt to obtain private information about other clients, when the X server replies to the client in an unexpected manner, or when the X client attempts to modify a global resource. The proposed solution involves a proxy X server handling all calls that the trusted X server would not deal with the same way as a general X server.

061226 'A Modular Covert Channel Analysis Methodology for Trusted DG/UX'
RA Kemmerer, T Taylor, *Apps 96 pp 224–235*

The paper describes a covert channel analysis of the Trusted Data General Unix (kernel) for the TCSEC B2 evaluation. The kernel is composed of about 170 subsystems, thus a modular approach of applying the analysis method (Shared Resource Matrix) for each subsystem and combining the results was used. Also, this allows for an easier re-analysis after changes in the design.

061227 'Deviant Byte Code: A Fundamental Threat to Java Security'
MD LaDue, *Information Security Bulletin v 2 no 2 (Mar 97) pp 17–26*

The author discusses the problem that Java class files can be created that pass the verifier but that could never have been compiled from Java source. He describes the class file structures in detail and shows how to insert arbitrary bytecode in a class file without changing its verifiability; discusses how exception handling can be manipulated and describes some simple deviant applets including Java viruses.

061228 'MITRE Technical Report 2547, Vol. II' (with preface and foreword)
LJ LaPadula, DE Bell, *Journal of Computer Security v 4 no 2/3 (Dec 96) pp 229–263*

This is a reprint of the classic report on the Bell-LaPadula model, with a historical preface by Jon Millen and a new foreword by Len LaPadula. This model played, and continues to play, an important role in the development of multilevel computer security. Between them, Bell and LaPadula generated several versions: volumes I, II, and III contained different, progressively more complex models. The later models reflected different design decisions, rather than being pure refinements of earlier ones. There was also a "Unified Exposition and Multics Interpretation."

061229 'Integrity and the Quality of Information: Part 1'
JR Lemieux, *Computer Fraud and Security Bulletin (3/97) pp 15–19*

The author argues that the definitions of integrity found in security policy models such as Biba and Clark-Wilson are at the wrong level of abstraction for many real world applications, where the concern is about data quality in the sense of accuracy, completeness, currentness and consistency; the models give only partial support for these attributes.

061230 'Strategic Directions in Computer Security Research'
TF Lunt, *Database 96 pp 1–10*

This invited talk elaborates on new directions in security research, and stresses the need of cooperation with the greater computer science community. It argues for modular systems with richer access control policies, and for affordability and scalability of the systems. It also suggests research to review ways of introducing security into a system by inserting security functions as 'wrappers' for critical system components.

061231 'Analytic performance comparison of transaction processing algorithms for the SINTRA replicated-architecture database system'
J McDermott, R Mukkamala, *Journal of Computer Security v 4 no 2/3 (Dec 96) pp 189–228*

This paper compares the performance of five of the most promising protocols for maintaining mutual consistency of multilevel database replicas. Its analytical model shows that although different protocols performed better under different conditions, the differences were relatively small. The protocols have distinct structural properties, and it is recommended that a choice between them be made based on either these properties or other factors rather than performance.

061232 'How Secure is Java?'
G McGraw, *Information Security Bulletin v 2 no 2 (Mar 97) pp 9–16*

The author provides an overview of some of the security holes discovered in Java implementations, and offers some advice for users.

061233 'Java Security and Type Safety'
G McGraw, E Felten, *Byte (Jan 97) pp 63–64*

The authors describe Java security measures, and specifically which mechanism is trusted to do what. Type safety is central, yet its implementation is complex and bugs have been found in the past.

061234 'The audit of NetWare 3.xx'
C Nelms, *Computer Audit Update (Jan 97) pp 18–22*

This article looks at NetWare security management tools, and particularly Bindview.

061235 'A Multilevel Security Model For Distributed Object Systems'
V Nicomette, Y Deswarte, *ESORICS 96 pp 80–97*

This paper presents a multilevel confidentiality model which has the same properties as Bell-LaPadula but is less restrictive. After describing some drawbacks of

Bell-LaPadula and some of its extensions the authors describe their model which is based on the notion of objects and activities; it is particularly adapted to distributed object systems and distinguishes between stateful and stateless objects. An example is given of an authorisation scheme in which illegal information flows are effectively prevented by the model.

061236 'Integrity Constraints in Federated Databases'
MS Olivier, *Database 96 pp 43–57*

Integrity in federated autonomous databases sharing data by reference is addressed. Consistency constraints in the object-oriented environment are discussed, and a method of optimising them to avoid expensive general enforcement is presented. The implementation of guarantees to ensure integrity is then discussed.

061237 'On the Interaction Between Role-Based Access Control and Relational Databases'
SL Osborn, LK Reid, GJ Wesson, *Database 96 pp 275–287*

Two experiments in interfacing a relational database to a role-based access control model are described. A relational database (IBM DB2/6000) with discretionary access control had a role-based access set up; then further roles were specified with resulting user-privilege pairs mapped in the database.

061238 'Access Control: The Neglected Frontier'
R Sandhu, *ACISP 96 pp 219–227*

This invited paper gives a perspective on mandatory and discretionary access control doctrines: it argues that they become discredited, but that no wide acceptance for other access controls like role and task-based ones has been gained. The author complains that access control has been neglected in recent security research.

061239 'Implementation Experiences and Prospects'
R Sandhu, L Notargiacomo, D Thomsen, J Worthington, *Database 96 pp 261–271*

Inputs to a panel discussion provide a cross section of the practical experience of three secure database vendors. Financial returns on MLS systems are abysmal, and the requirements of government and commercial customers are almost disjoint. One vendor has managed to get some commercial return on a B1 database by running it on a standard C2 operating system; its control features are still of some value to companies.

061240 'Role Hierarchies and Constraints for Lattice-Based Access Control'
R Sandhu, *ESORICS 96 pp 65–79*

The author describes how different variations of the lattice-based access control model can be simulated using the role-based access control model. This is achieved by changing the role hierarchy and defining appropriate constraints in the latter.

061241 'SIGMA: Security for Distributed Object Interoperability Between Trusted and Untrusted Systems'
EJ Sebes, TCV Benzel, *Apps 96 pp 158–168*

An architecture for integrating security techniques into distributed environments based on CORBA is discussed, together with ways to allow the exchange of object-oriented services among domains with different security policies and mechanisms. The idea is to facilitate CORBA-based interaction in multilevel systems. Much of the approach is based on firewall-type techniques with single points of access to domains.

061242 'Detecting illicit leakage of information in operating systems'
SP Shieh, V Gligor, *Journal of Computer Security v 4 no 2/3 (Dec 96) pp 123–148*

This paper addresses the problem of covert channels, which may exist in spite of adherence to an access control policy such as Bell-LaPadula. While some covert channels can be closed, the rest must be audited; the paper discusses how audit collection

mechanisms and analysis tools should be designed. Secure Xenix is used as the reference example; sender and receiver programs are listed that use disk-inode-space and file-table error return variables to communicate, and a sample audit trail is given.

061243 'Security Enforcement in the DOK Federated Database System'
Z Tari, G Fernandez, *Database 96 pp 23–42*

The authors present a federated database system called the Distributed Object Kernel. Their security model integrates access control models of autonomous databases, operates on virtual objects as an aggregation of existing local objects, and provides for explicit mapping of both mandatory and discretionary access control. 'Coordination agents' are set to delegate functions to specific 'task agents' that enforce the federated security policies. The aggregation aspects are reviewed in some detail.

061244 'Security Issues for Data Warehousing and Data Mining'
BM Thuraisingham, *Database 96 pp 11–20*

This invited talk reviews data warehousing and problems of inconsistent policies for integration of heterogeneous databases, and points out other security relevant issues. Data mining applications to intrusion detection and inference are also discussed.

061245 'An Object-Oriented Database Architecture for providing Security in Cyberspace'
RP van de Riet, E Gudes, *Database 96 pp 120–144*

The protection properties of a proprietary object-oriented knowledge-based system are discussed in a home banking model case. The paper argues for a unique 'alter-ego' concept of an identifier and personal information object.

061246 'Extending the schematic protection model II: revocation'
V Varadharajan, *Operating Systems review v 31 no 1 (Jan 97) pp 64–77*

Following on from **032229**, this paper shows how Sandhu's schematic protection model can be extended to deal with the revocation of privileges in a reversible way; this enables its safety properties to be preserved.

061247 'Extending the schematic protection model II: revocation'
V Varadharajan, C Calvelli, *Computers and Security v 15 no 6 (1996) pp 525–536*

This article is substantially the same as the one above, but has an expanded section on the details of handling revocation tickets.

061248 'Support for Joint Action Based Security Policies'
V Varadharajan, P Allen, *ACISP 96 pp 207–218*

The authors discuss some aspects of designing joint action based authorisation policies (dual control). Some attributes of these schemes are introduced, and three schemes on a hypothetical medical example are discussed. One involves temporary delegation with tickets, the others a central authority — either a dedicated one or just that performing the relevant action. The implications of these schemes for trust in components are reviewed.

061249 'A sound type system for secure flow analysis'
D Volpano, C Irvine, G Smith, *Journal of Computer Security v 4 no 2/3 (Dec 96) pp 167–187*

This paper describes how to embed information flow into an inference system that manipulates fragments of program text. The programs are written in a special purpose, but relatively conventional, programming language. The paper encodes security (or integrity) information as types for expressions, variables, and commands. Rules in the inference system enumerate the type of a given program structure as a function of the constituent parts of that program structure. A noninterference theorem shows that the result (but not the timing) of a computation in a well-typed program is unaffected by computations at incomparable or dominating levels. This establishes the soundness of Denning's lattice model.

3 Security Management and Policy

061301 'Open for Business — Securely'
D Adams, *Computers and Security v 15 no 8 (1996) pp 673–682*

The author describes the Open Group's 'Baseline Security 96' standard which contains a number of recommendations on things like access controls, security manuals, audit and trusted recovery.

061302 'Money and the Internet: a strange new relationship'
H Anderson, *IEEE Spectrum v 34 no 2 (Feb 97) pp 74–76*

The author talks about e-cash and the Internet.

061303 'Internet — Virusnet?'
D Aubrey-Jones, *Network Security (Feb 97) pp 15–19*

The nine most common viruses in the UK in 1995 were boot sector viruses, but during the first half of 1996 the Winword 'Concept' macro virus shot to second place. In the USA, it is in top place. The growth of the Internet should assure that Word and ActiveX viruses will predominate in future.

061304 'Lacking the e-safe'
RW Baldwin, CV Chang, *IEEE Spectrum v 34 no 2 (Feb 97) pp 40–46*

This is a management level tutorial on cryptology written by two people at RSADSI.

061305 'Over and Out: Signals Intelligence (Sigint) in Hong Kong'
D Ball, *Intelligence and National Security v 11 no 3 (July 96) pp 474–496*

This history of UK sigint operations in Hong Kong relates how successive installations there targeted Japanese traffic in the 1930's, and Chinese after WW2. Technical facilities grew from simple MW/HF antennas through equipment to intercept satellite communications and missile test telemetry. Some information on Chinese military satellites is included.

061306 'The Fundamentals of Computer Forensics'
J Bates, *International Journal of Forensic Computing; part 1, v 1 no 1 (Jan 97) pp 4–5; part 2, v 1 no 2 (Feb 97) pp 3–4*

The author discusses the basics of seizing and preserving computer data for use in evidence, and suggests a procedure for sealing a second copy of the evidence in the owner's presence when the machine is seized as a precaution against claims of tampering.

061307 'Cyberspace and the legal woes of employers'
A Bequai, *Computer Audit Update (Mar 97) pp 33–36*

The author talks about some of the legal problems facing US employers as a result of computer security vulnerabilities.

061308 'The US IT security market and its legal trappings'
A Bequai, *Computer Audit Update (Feb 97) pp 18–21*

Pitfalls for computer security vendors in the USA include privacy concerns, labour unions, health and safety regulations, anti-discrimination bodies, strict product liability laws and anti-trust provisions.

061309 'Legal Issues in Computer Security — A Report from the United States (part 2)'
R Bigelow, *Computer Law and Security Report v 13 no 2 (Mar-Apr 97) pp 87–95*

The author talks about privacy law, computer abuse, personal liability, defamation, failure to observe standards, and other 'computer' hazards of business in the USA.

061310 'Chip Theft: Analysing the Risks and Practical Solutions'
C Blackwell, *Computer Fraud and Security Bulletin (Jan 97) pp 7–11*

This article discusses what companies can do about computer chip theft.

061311 'Netegrity's Sidewinder software lets net managers get control of security'
L Bruno, *Data Communications International (Jan 97) pp 84–86*

This article describes a Windows NT product that centralises the management of enterprise-wide security via a web-like interface.

061312 'Managing Network Security'
F Cohen, *Network Security: part 1, Dec 96 pp 9–11; part 2, Jan 97 pp 8-11; part 3, Feb 97 pp 12–15; part 4, Mar 97 pp 8–10*

The author discusses some network security management issues such as the mix of infrastructure-based and host-based protection, the balance between integrity and confidentiality protection, and how to explain the problems to managers.

061313 'How Jim Bamford Probed the NSA'
P Constance, *Cryptologia v XXI no 1 (Jan 97) pp 71–74*

This tells the story of how Jim Bamford gathered the material for his book, 'The Puzzle Palace'; his sources included personal papers of former employees that had been donated to libraries, a Justice Department investigation, and the NSA's own personnel newsletter.

061314 'Cyber Threat Challenges Intelligence Capability'
C Couvault, *Aviation Week and Space Technology v 146 no 6 (1/2/97) pp 20–21*

This article reports an air warfare symposium at which the director of the NSA claimed that the United States' ability to network computers had far outpaced its ability to protect them from logical attack. He emphasised the need to integrate operations, intelligence and communications, so that intelligence professionals could participate alongside warfighters.

061315 'The BRUSA agreement of May 17, 1943'
Cryptologia v XXI no 1 (Jan 97) pp 30–38

This reproduces the recently declassified wartime agreement between Britain and the USA on sharing communications intelligence. It deals not just with the division of labour, but also with security precautions to be taken with ULTRA decrypts.

061316 'Council of Europe Activities Related to Information Technology, Data Protection and Computer Crime'
P Csonka, *Information & Communications Technology Law v 5 no 3 (96) pp 177–196*

The author describes a number of activities undertaken since 1989 by the European Commission to analyse computer crime problems in Europe, help develop a unified approach under procedural law to issues such as the admissibility of evidence, to harmonise substantive computer crime provisions, and to safeguard the privacy of individuals.

061317 'Verbraucherschutz im Internet'
H Damker, G Müller, *Datenschutz und Datensicherheit v 21 (Jan 97) pp 24–29*

The authors attempt a risk analysis of the threats to individual rights arising from the net. They cover privacy, anonymity, and profiling; they describe some countermeasures, including PGP, SSL and anonymous remailers.

061318 'Informations- und Kommunkationsdienste-Gesetz — IuKDG — Beschlußdes Bundeskabinetts'
Datenschutz und Datensicherheit v 21 (Jan 97) pp 38–45

This is the text of Germany's proposed new law on communications services, which will regulate digital signatures, the licensing of trusted third parties, and so on. All certificates must bear the name of the owner, who must be well identified; there is no provision for role certificates to have legal force.

061319 'Verordnung zur Digitalen Signatur (Signaturverordnung — SigV)'
Datenschutz und Datensicherheit v 21 no 2 (Feb 97) pp 102–106

This is the text of the German regulation on digital signatures as enacted in January 1997.

061320 'Kryptoregulierung — Jetzt auch in Deutschland?'
R Dierstein, *Datenschutz-Berater v 21 no 2 (17/2/97) pp 3–6*

At least three German ministries are working hard at plans to regulate all cryptography; the possible libertarian and economic consequences of this are discussed.

061321 'Old Laws, New Crimes ... and a Shrinking Planet'
M Duncan, *International Journal of Forensic Computing v 1 no 3 (mar 97) pp 10–12*

This article presents the Royal Canadian Mounted Police's view of forensic computing and its problems. They consider themselves to have been generally successful, but there are increasing numbers of court challenges to the integrity and authenticity of computer evidence, as well as problems with training and jurisdiction.

061322 'Internet Law'
R Drurie, *Computer Law and Security Report v 13 no 1 (Jan-Feb 97) pp 29–33*

The author talks about the background to the recent dispute over domain names and the current policy of the name service contractor, Network Solutions, on allocating them.

061323 'Anonymity in the Global Network: A First World Dream'
B Dwan, *Computer Fraud and Security Bulletin (Mar 97) pp 12–14*

A number of social forces are pushing in the direction of anonymity in digital transactions; these range from the nuisance of junk email through the dominance of 'first world culture' in computer science departments and universities.

061324 'The Security Implications of the Digital Diary'
B Dwan, *Computer Fraud and Security Bulletin (Feb 97) pp 9–10*

Many personal organisers offer some kind of password protection, but this may be vulnerable to attacks using their PC backup and editing features.

061325 'Telediesntdatenschutz'
S Engel-Flechsig, *Datenschutz und Datensicherheit v 21 (Jan 97) pp 8–16*

A proposed German law regulating cryptography, digital signatures, law enforcement access to telecommunications services, and the use of anonymity is explained by one of its authors. The alleged goal is to provide a unified federal framework for regulating multimedia.

061326 'Naval Enigma: An Astonishing Blunder'
R Erskine, *Intelligence and National Security v 11 no 3 (July 96) pp 468–173*

The German naval enigma 'Süd', known as Porpoise, Grampus and Trumpeter to Allied codebreakers and used in the Black Sea and the Mediterranean, continued to use double enciphered message indicators until June 1944 — long after other nets had abandoned this unsafe practice. However, Bletchley did not attack it until twelve months after its introduction. The Germans' blunder is ascribed to the lack of a central crypto unit in the Wehrmacht.

061327 'The First Naval Enigma Decrypts of World War II'
R Erskine, *Cryptologia v XXI no 1 (Jan 97) pp 42–46*

This describes the initial breaks into German naval traffic in 1941, which involved captures and some bombe work.

061328 'Smart Card Tutorial'
D Everett, *Smart Card News; part 1: v 6 no 1 (Jan 97) pp 16–19; part 2: v 6 no 2 (Feb 97) pp 36–39*

These articles provide a simple overview of the basic communications protocols used between smartcards and card readers.

061329 'Comeback für Road Pricing'
S Felixberger, *Datenschutz-Berater v 21 no 3 (14/3/97) pp 3–4*

Germany intends to replace commercial vehicle taxation with road tolls; this raises a number of data protection issues, which are discussed here.

061330 'Neue US-Exportregeln für Kryptoprodukte'
S Felixberger, *Datenschutz-Berater v 21 no 1 (15/1/97) pp 1–4*

This presents a German view of recent developments in US crypto law, and points out that although not so well known, German export regulations have a very similar effect.

061331 'Why Safeguard Information? — A Finnish Perspective'
T Finne, *Computer Audit Update (Jan 97) pp 10–17*

The author provides a Finnish perspective on information security, citing surveys of corporate attitudes, investment and so on.

061332 'Case Study — Operation Cybertrader'
P Ford, P Verreck, *International Journal of Forensic Computing v 1 no 1 (Jan 97) pp 7–9*

This article describes the procedures used to secure evidence in a recent UK prosecution for child pornography; it argues for police use of professional computer forensics experts with dedicated equipment.

061333 'European Initiatives in Privacy and Data Protection'
E France, *Computer Fraud and Security Bulletin ((Jan 97) pp 12–16*

Britain's Data Protection Registrar discusses the 1995 EU directive on data protection and explains why implementing this by regulations under the European Communities Act on 1972, rather than by new primary legislation, would give rise to complexities and contradictions in the protection regime. She also suggests the form that new legislation should take in order to make her business more streamlined and effective.

061334 'Security Issues in the Virtual Corporation'
RL Frank, *Computers and Security v 15 no 6 (1996) pp 471–476*

The author talks about the security problems created by outsourcing.

061335 'Real World Anti-Virus Product Reviews and Evaluations'
S Gordon, R Ford, *Network Security: part 1, Dec 96 pp 14–18; part 2, Jan 97 pp 11–18*

The authors discuss the drawbacks of current methods for evaluating anti-virus software and suggest that plans to incorporate antivirus product testing in ITSEC may be of value.

061336 'The US Cryptographic Export Debate — Round Five?'
W Hancock, *Network Security (Mar 97) pp 6–7*

The author describes successive US government attempts to control encryption, from CCEP through Clipper to TTPs.

061337 'Israel — Computer Forensics the Hard Way'
R Hatley, *International Journal of Forensic Computing v 1 no 2 (Feb 97) pp 5–7*

This article describes the Israeli police's computer forensics team and some of the problems they face, from multiple alphabets through a law that forces them to hand seized computers back to their owners after 48 hours unless evidence of a crime is found

in them. It also describes a technique for finding hidden disk partitions, even when the BIOS settings have been changed.

061338 'The Internet and Computer Forensics'
R Hatley, *International Journal of Forensic Computing v 1 no 1 (Jan 97) pp 11-12*
This article describes some of the problems inherent in gathering evidence of a network intrusion or attempted intrusion.

061339 'Year 2000 — A Real IS Security Issue'
EB Heinlein, *Computers and Security v 15 no 6 (1996) pp 499–500*
No-one yet uses the date change to 2000 as a factor in testing disaster recovery plans, despite its being the biggest imminent disaster of all.

061340 'Blackmail'
International Journal of Forensic Computing v 1 no 2 (Feb 97) pp 8–9
This article describes a successful investigation of blackmail in the UK which turned on reconstructing deleted word processing files from a hard disk.

061341 'Datenschutz und Telefax'
U Jürgens, *Datenschutz-Berater v 21 no 2 (17/2/97) pp 8–10*
German data protection officials have issued guidelines on fax security that, for example, forbid government officials from faxing citizens' personal information such as tax and medical files to third parties, except in exceptional circumstances, or when encryption is used.

061342 'The future of electronic money: a regulator's perspective'
EW Kelly, *IEEE Spectrum v 34 no 2 (Feb 97) pp 21–22*
A US Federal reserve governor gives his view on electronic cash: he is not alarmed by developments to date, as only stored value cards are really any different from existing banking products — and these are unlikely to get big enough to threaten the financial system.

061343 'Establishing a Network Security Programme'
GJ Kovacich, *Computers and Security v 15 no 6 (1996) pp 486–498*
This is a checklist for setting up a corporate network security programme.

061344 'Smart Card Security'
P Krauss, *Information Security Bulletin v 2 no 2 (Mar 97) pp 37–38*
The author considers some of the regulatory and trust problems of introducing smartcards based systems.

061345 'A Security Officer's Workbench'
FK Lam, D Longley, *Computers and Security v 15 no 8 (1996) pp 695–705*
This journal version of **033341** describes a hypertext based system for centralising security relevant information in a company.

061346 'Internet Regulation in Singapore'
TK Leng, *Computer Law and Security Report v 13 no 2 (Mar-Apr 97) pp 115–119*
This article reviews Singapore's licensing and regulation systems for Internet service providers.

061347 'On the Role of Information Security in Corporate Governance'
K Lindup, *Computers and Security v 15 no 6 (1996) pp 477–487*
This article talks about problems with translating corporate policy into fielded controls, with emphasis on new technologies such as speech processing and groupware. The general trend is that as business processes are automated and distributed, the security perimeter is diffused.

061348 'Airline passengers to be subject to database monitoring'
W Madsen, *Computer Fraud and Security Bulletin (Mar 97) pp 7–8*

The FAA and a White House commission have recommended that a database be created of all airline passengers, with biometrics (including not just a photo but also body X-rays), flying patterns, criminal record, credit information and links to entries for travel partners. This would be used to identify passengers fitting a terrorist profile; such people would be subjected to heightened security checks. The American-Arab Anti-Discrimination Committee has reported many incidents where innocent passengers have been harassed by airlines that have implemented some of these recommendations.

061349 'Information warfare: the sequel'
W Madsen, *Computer Fraud and Security Bulletin (Feb 97) pp 5–6*

The US Defense Science Board has recommended that $3 bn be spent over the next five years to counter information warfare threats. Opponents claim that this is simply an attempt to create a post-cold-war bogeyman and increase surveillance of domestic traffic.

061350 'United States Remains Adamantly Opposed to Data Protection'
W Madsen, *Computer Fraud and Security Bulletin (Dec 96) pp 6–10*

This article describes the US input to a data protection officials' meeting in Canada in September 1996 and other countries' negative reaction to it. It foresees a crunch in 1998 when the directive's implementation will cut flows of personal information between the EU and the USA.

061351 'Is the threat of the high-tech computer hacker an exaggerated one, or was there ever a need for the Computer Misuse Act 1990?'
W Madsen, *Computer Fraud and Security Bulletin (Dec 96) pp 11–18*

The author describes the hysteria that led to the passage of the Computer Misuse Act in Britain, and argues that most computer crimes could have been prosecuted under existing provisions for crimes such as theft and criminal damage.

061352 'Web security: how much is enough?'
V McCarthy, *Datamation (Jan 97) pp 112–117*

A task force of people from some 60 US companies has drafted recommendations for assessing the security risks of a corporate web site, in an attempt to set a duly diligent level of protection.

061353 'Legal Ethics and the Internet: A US Perspective'
JM McCauley, *Computer Law and Security Report v 13 no 2 (Mar-Apr 97) pp 110–114*

There is a dispute in the US legal profession about whether standards of professional care require that email messages about client affairs be encrypted; some people argue that failure to encrypt might be negligent or even constitute a waiver of professional privilege.

061354 'Crime and prevention: a Treasury viewpoint'
SE Morris, *IEEE Spectrum v 34 no 2 (Feb 97) pp 38–39*

The director of FinCEN, a US government agency responsible for fighting money laundering, describes US efforts to ensure that electronic payment systems do not make life easier for white collar criminals.

061355 'Schlüsselgenerierung in Trust Centern?"
R Nehl, *Datenschutz und Datensicherheit v 21 no 2 (Feb 97) pp 100–101*

The author discusses some of the issues of trust, evaluation and accreditation involved in setting up CAs.

061356 'Intellectual Property Law'
S Newman, *Computer Law and Security Report v 13: part 1, no 1 (Jan-Feb 97) pp 22–28; part 2, no 2 (Mar-Apr 97) pp 96–101*

The author describes how moral and adaptation rights originated historically, how they operate in various countries, and how they are being adapted to digital technology.

061357 'The Changing Face of Information Technology Security'
S Orlowski, *ACISP 96 pp 1–13*

This paper reviews some of the recent issues that are arising in data protection, crypto policy and related issues. It compares the OECD's 1980 "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" with the 1992 "Guidelines for the Security of Information Systems". It emphasises the importance of authentication rather than confidentiality, and urges academia and computer industry to develop systems that can only be used for the former so that the restrictions currently applied to export and so on could be relaxed. Finally, it talks about the current crypto policy initiatives in the USA, the UK, France and Australia.

061358 'For Whom the Modem Tolls: The Travails of America Online'
J Osen, *Network Security (Mar 97) pp 17–19*

The author describes an FBI operation against America Online in which agents posed an minors and had subscribers send them pornography or solicit sexual encounters. He also talks about some service outages and copyright disputes.

061359 'Obscenity on the Internet'
R Parry, A Lee, A Russell, *Computer Audit Update (Mar 97) pp 37–39*

The authors describe existing UK laws that can be used to prosecute electronic distributors of obscene material, and the due diligence measures that might be taken by employers and network providers.

061360 'Cryptography, trusted third parties and key escrow'
SJD Phoenix, *BT Technology Journal v 15 no 2 (Apr 97) pp 45–62*

This paper gives a basic introduction to cryptography and then goes on to talk about the UK government's proposed key escrow scheme.

061361 'Kommunikationstechnik als Quelle für Wirtschaftspione'
T Pleil, *Datenschutz-Berater v 21 no 1 (15/1/97) pp 4–6*

The number of cases of economic espionage has trebled in the USA in the last three years; such activities are considered to be a problem by an increasing number of developed countries. Signals intelligence is reckoned to amount for eighty percent of the total.

061362 'Preparing for the worst'
CB Powers, *IEEE Spectrum v 33 no 2 (Dec 96) pp 49–54*

The author describes a large number of things that can go wrong with systems when a disaster such as a flood or hurricane strikes, and discusses how to prepare for them.

061363 'Das Signaturgesetz'
A Roßnagel, *Datenschutz und Datensicherheit v 21 no 2 (Feb 97) pp 75–81*

The author describes the proposed German law on digital signatures which involves CA licensing and various other provisions. A number of ambiguities are pointed out.

061364 'Datenschutz un der liberalisierten Telekommunikation'
P Schaar, *Datenschutz und Datensicherheit v 21 (Jan 97) pp 17–23*

The official responsible for data protection in Hamburg explains that Germany's proposed new telecommunications law will significantly change the data protection rights that individuals have; furthermore, public and private networks will be treated differently.

061365 'The Internet Rules but the Emperor has no Clothes'
R Schell, *Apps 96 pp xiv–xix*

In this invited talk, a senior manager at Novell identifies a number of issues that need to be tackled in securing the net. Trusted path is just as important as cryptography; so is trusted distribution and a framework for customer responsibility.

061366 'Security Management for Administration and Control of corporate-wide, diverse Systems'
G Schimpf, *ACM SIGSAC Review v 15 no 1 (Jan 97) pp 4–10*

This article describes an MVS software package designed to provide centralised security management for a wide range of platforms such as OS/2 and Unix as well as MVS. It reports an implementation in a large bank with 900 servers, 50,000 computers and 28,000 users.

061367 'Why Cryptography is Harder than it Looks'
B Schneier, *Information Security Bulletin v 2 no 2 (Mar 97) pp 31–36*

The author reviews some of the difficulties of implementing systems that use cryptography effectively.

061368 'Future Imperfect'
Secure Computing (Feb 97) pp 18–25

This article talks about a number of recent security product developments and reports market studies of e-cash and Java.

061369 'SALSA: A Method for Developing the Enterprise Security Architecture and Strategy'
J Sherwood, *Computers and Security v 15 no 6 (1996) pp 501–506*

Most security solutions are acquired and installed on a tactical basis; the author describes a method he has developed to try to do it strategically.

061370 'Trusted third parties in electronic commerce'
PJ Skevington, TP Hart, *BT Technology Journal v 15 no 2 (Apr 97) pp 39–44*

This paper talks about certification hierarchies and the liability of CAs.

061371 'Encryption for a small planet'
T Stork, *Byte (Mar 97) pp 111–114*

This article describes the quite diverse strategies adopted by Netscape, Lotus, Sun, Qualcomm, PGP and Hewlett-Packard to cope with US export restrictions on encryption products.

061372 'Öffnet ActiveX Hackern Tür und Tor?'
D Stricharz, *Datenschutz-Berater v 21 no 3 (14/3/97) pp 6–8*

This article reports an demonstration attack on a banking system carried out by Hamburg hackers using an ActiveX control. Authenticode does not provide a solution, as it certifies merely the code's origin and not its function. These products, plus the loosening of Java's 'sandbox', have the effect of dumping responsibility on the user.

061373 'The economics of e-cash'
M ter Maat, *IEEE Spectrum v 34 no 2 (Feb 97) pp 68–73*

An ABA economist assesses whether ecash systems could be financed from the float; potential difficulties are in getting critical mass and in reassuring customers. In the US, for example, the Federal Deposit Assurance Corporation has ruled that e-cash not tied to a deposit account will not be insurable. However, governments are bound to have a role, and may issue e-cash themselves — it could be a natural outgrowth of welfare benefit payment systems.

061374 'Breakthroughs in Standardisation of IT Security Criteria'
E Troy, *ACISP 96 pp 108–120*

This talk starts by motivating the need for IT security criteria including the internationalisation of the computer market, the need for successors to earlier criteria, and the requirement for a clear vocabulary and syntax for describing security requirements. It gives a brief history of security criteria and provides an overview of Common Criteria which is seen as the major breakthrough in in the field of IT security.

061375 'Electronic Money and Key Management from Global and Regional Points of View'
S Tsujii, *Asiacrypt 96 pp 173–184*

Using electronic money as an example, the author contends that trans-national information networks will bring about a global harmonisation of economic systems and legal institutions.

061376 'Data Warehouse Control and Security'
S Warigon, *Information Security Bulletin v 2 no 2 (Mar 97) pp 41–50*

The author proposes a methodology for assessing the threats to data warehousing systems, and selecting, implementing and evaluating protective mechanisms.

061377 'Constructing Difficult-to-Guess Passwords'
CC Wood, *Information Security Bulletin v 2 no 2 (Mar 97) pp 39–40*

The author discusses a number of tricks that can be used to construct passwords that are easy to remember but hard to guess, and the need to drum these into users.

061378 'Critical Infrastructure Protection'
CC Wood, *Computer Fraud and Security Bulletin (Mar 97) pp 8–9*

The US Presidential Commission on Critical Infrastructure Protection was set up in July 1996 and now wants utility and infrastructure companies to share information on their information security vulnerabilities with it. This is getting a mixed reception. Meanwhile the Justice Department has convinced SWIFT to upgrade its security, and the NSA is monitoring major Internet nodes.

061379 'Information Security: Are We Losing the Game?'
CC Wood, *Computer Fraud and Security Bulletin (Jan 97) pp 5–6*

In addition to creating jurisdictional problems, the Internet facilitates privacy infringement: some US employers now read all the usenet postings of prospective hires to find out their proclivities.

061380 'Recent Crypto-Process Developments: Highlights from the 1997 RSA Conference'
CC Wood, *Computer Fraud and Security Bulletin (Mar 97) pp 10–11*

The author talks about some of the talks at the RSA conference.

4 Formal Methods and Protocols

061401 'Using Formal Methods to Cultivate Trust in Smart Card Operating Systems'
MI Alberda, PH Hartel, EK de Jong, *Cardis 96 pp 111–132*

The formal specification of the core of a proprietary systems programming language for smartcards is given. Smartcard software would come through a three-layer architecture, and the formal specification could support development of application as well as systems code.

061402 'Innovative Secure Payments on the Internet using the German Electronic Purse'
B Althen, G Enste, B Nebelung, *Apps 96 pp 88–93*

This article describes the principles and protocols of the German 'Geldkarte' — a eurocheque card with an electronic purse chip. Both customers and merchants use cards, as the transactions are off-line, encryption is done with single and triple DES, MAC with CBC and CFB single DES. Transactions are anonymous with the merchant, but not with the bank clearing centre. The card's use can be extended to Internet payments denominated in Deutschmarks.

061403 'NetCard — A Practical Electronic-Cash System'
R Anderson, C Manifavas, C Sutherland, *Protocols 96 pp 49–57*

This article describes a protocol for micropayments; users create sticks of electronic coins by repeated hashing and then authenticate the top coin using a digital signature or some other mechanism such as SET. They can then spend the coins one by one to pay for services such as network bandwidth and publication page charges. The recipient can finally bill for the amount spent, having the revealed coins as evidence in case of a dispute.

061404 'Towards a More Secure Internet'
R Atkinson, *IEEE Computer v 30 no 1 (Jan 97) pp 57–61*

The author describes current efforts to retrofit encryption to the existing Internet protocol suite, and to incorporate it into IPv6.

061405 'On Password-Based Authenticated Key Exchange Using Collisionful Hash Functions'
S Bakhtiari, R Safavi-Naini, J Pieprzyk, *ACISP 96 pp 299–310*

An attack on the password-based authenticated key exchange protocol of Anderson and Lomas in **033601** is presented: the compromise of an old session key enables the password to be found. An improved version of the scheme is presented, which involves passing the final session key through a one-way hash function. Another two key exchange protocols using passwords are also provided.

061406 'On Selectable Collisionful Hash Functions'
S Bakhtiari, R Safavi-Naini, J Pieprzyk, *ACISP 96 pp 287–298*

The authors present some problems with a collisionful hash function scheme by Gong (**043414**) that can result in an attack: the attacker can forge a checksum of a message given reasonable computing power. The scheme would resist all possible attacks if the password space is large enough, but this was not its design goal. Two alternative improvements are suggested.

061407 'A Framework for Design of Key Establishment Protocols'
C Boyd, *ACISP 96 pp 145–157*

This paper classifies authentication protocols according to whether the recipients chose the identity of the other participants or not, and whether they contributed to the freshness or not. This gives four generic classes of protocol, and an example is given

of each of them. This framework is used to design new protocols suitable for given environments.

061408 'Systematic design of key establishment protocols based on one-way functions'
C Boyd, A Mathuria, *IEE Proceedings on Computers and Digital Techniques v 144 no 2 (Mar 97) pp 93–99*

The authors analyse the confidentiality and authentication channels in a 1989 protocol of Gong, and show that the second user has no real assurance of key freshness; the first user can force him to accept an old session key. Their analysis finds an already known attack on a protocol of Bull, Gong and Sollins (**021202**), and a number of new and powerful attacks on lightweight versions of IBM's KryptoKnight protocols. These problems stem from binding the confidentiality and authentication channels too closely together. Finally, they propose better protocols for standard authentication and conference key setup using hash functions.

061409 'Digital Payment Systems with Passive Anonymity-Revoking Trustees'
J Camemisch, U Maurer, M Stadler, *ESORICS 96 pp 33–43*

The authors propose the use of a trusted third party in payment systems to allow the revocation of anonymity of the participants in case of need. They describe a protocol that can be used as alternative to the challenge/response techniques of other payment systems to solve the same problem. The peculiarity of the trusted party introduced in this paper is her passivity; she does not need to be involved in all transactions, or to participate in the opening of accounts.

061410 'Key Escrow in Mutually Mistrusting Domains'
L Chen, D Gollmann, CJ Mitchell, *Protocols 96 pp 139–153*

Two key escrow systems for international use in such domains are presented. One scheme is based on the escrow architecture from **043616**, the other on some ideas from **044417**. All third parties and key users jointly generate the key in the first scheme; a transfer of key shares followed by verification is used in the second. One of the primary aims of both schemes is to complicate any attempt of the users to subvert the escrowed key and use a 'shadow key'; another is to escrow the key with third parties in every domain involved.

061411 'Tailoring authentication protocols to match underlying mechanisms'
LD Chen, D Gollmann, C Mitchell, *ACISP 96 pp 121–133*

The fundamental components of authentication protocols are cryptographic mechanisms and time varying parameters such as clocks, nonce generators and sequence number generators. A typical authentication protocol uses at least one mechanism of each category. A designer will tailor her protocol to the strength of the available mechanism, while properties of the environment and the resources of authenticating entities affect the design too. This paper examines the ISO/IEC 9798 protocols in this context, and shows that in some environments these requirements may be relaxed. Finally, it suggests alternatives which are less demanding on the mechanisms.

061412 'A Certification Scheme for Electronic Commerce'
B Crispo, M Lomas, *Protocols 96 pp 19–32*

The authors discuss how key certification services can be made robust against undetected failure. They present a design in which separation of duty ensures that at least two entities out of the three (user, certification authority and a separate revocation authority) have to collaborate to enforce a change in a certificate or in the evidence. The design lays great emphasis on evidence being fully verifiable, with hash chaining to prevent re-ordering and other manipulation of certificates and logs.

061413 'Why Isn't Trust Transitive?'
B Christianson, WS Harbison, *Protocols 96 pp 171–176*

The authors discuss trust transitivity aspects. Many approaches in applying public-key cryptography and delegating certain functions to third parties rest on unexamined and often incorrect trust assumptions, and the entities' consent is often lacking. The importance of analysing beliefs held by entities about each other, and the basis of such beliefs, is stressed.

061414 'Another approach to software key escrow encryption'
E Dawson, J He, *ACISP 96 pp 87–95*

This paper points out new shortcomings of two software key escrow systems and proposes an improved system that combines their advantages with some new features. It allows negotiation of the common key, identification of principals by the law enforcement agency, and controlled wiretaps. As with the previous systems, it relies on the assumption that there is some secure code in the software which cannot be bypassed.

061415 'Security for Mobile Agents: Authentication and State Appraisal'
WM Farmer, JD Guttman, V Swarup, *ESORICS 96 pp 118–130*

The paper addresses the problems of authentication and authorisation in the special case of mobile agent technology. They discuss some of the problems of defining a logic that formalises the delegation and authorisation relationships involved.

061416 'Schlüsselgenerierung in Trust Centern?'
H Federrath, *Datenschutz und Datensicherheit v 21 no 2 (Feb 97) pp 98–99*

The author discusses the problems of generating signature keys centrally or locally; the ability of the trust centre to forge signatures must be considered along with the physical security of equipment and the difficulty of generating good random numbers. He suggests that ideally, signing keys should be generated in an interactive process involving a number of parties. Respecting mistrust will be the critical success factor.

061417 'Multi-Application Smart Cards and Encrypted Data Processing'
JD Ferrer, *Cardis 96 pp 145–156*

The author argues for ways to run some applications outside a smartcard, while processing encrypted data through privacy homomorphisms. A privacy homomorphism is presented that supports addition, subtraction, multiplication and in a sense division as well.

061418 'Traceable e-cash'
P Gemmell, *IEEE Spectrum v 34 no 2 (Feb 97) pp 35–37*

The author describes how e-cash protocols may be endowed with escrow mechanisms.

061419 'Structuring and Visualising an IC-card Security Standard'
H Glaser, PH Hartel, EK de Jong Frz, *Cardis 96 pp 89–110*

A way to visualise some protocols in the CEN inter-sector electronic purse standard draft is discussed. This should ease viewing the manipulation of state in protocols.

061420 'Investigation of non-repudiation protocols'
Y Han, *ACISP 96 pp 38–47*

This paper reviews the main classes of non-repudiation protocols and underlines the limitations of each class. It defines a model for non-repudiation protocols without a Trusted Third Party (TTP) that uses a public access system — a kind of black box that cannot be modified by the user. It also describes a protocol that uses a time stamp chain to ensure entities respond to the received messages and hence provide the required evidence that can be presented to an adjudicator in the case of dispute. The protocol provides equal protection for transmitter and receiver.

061421 'Replicating the Kuperee authentication sever for increased security and reliability'
T Hardjono, J Seberry, *ACISP 96 pp 14–26*

This paper describes the use of a threshold scheme in an authentication service (Kuperee). This helps to overcome problems associated with low availability of servers and the risk that their key material might be compromised. The system has 2 phases: in key generation phase, the Key Distribution Centre (KDC) generates a session key pair and distributes the private part of the pair among servers. In the authentication phase, a client can authenticate itself by contacting at least t out of n servers to get a session key. The paper concludes with a comparison of this scheme and other similar approaches.

061422 'Design Choices for Symmetric Key Based Inter-domain Authentication Protocols in Distributed Systems'
M Hitchens, V Varadharajan, *Apps 96 pp 105–116*

The authors discuss design choices of inter-domain authentication in Kerberos type systems. The presented protocols differ in the workload of the client of the ticket granting server. The assumptions of the design are outlined; both the number of messages and their eventual reduction are discussed.

061423 'Authenticated Multi-Party Key Agreement'
M Just, S Vaudenay, *Asiacrypt 96 pp 36–49*

A generalisation of the Burmester-Desmedt scheme from **032605** is presented. An attack against the authenticity of one specific Burmester-Desmedt scheme is outlined, some attacks against the generalised scheme are analysed, and two two-party key agreement protocols are presented. Four attacks are presented against some other two-party protocols. All the key agreement schemes involved are Diffie-Hellman based.

061424 'Authenticating Outputs of Computer Software Using a Cryptographic Coprocessor'
J Kelsey, B Schneier, *Cardis 96 pp 11–24*

An idea for using tamper-resistant hardware for the certification of software outputs and software usage metering is described. The hardware box contains only a part of the software, as the rest can be stored on the main computer. The communication of certified output can be electronic or manual; ways to implement other features are discussed.

061425 'Verifying the Correctness of Cryptographic Protocols Using "Convince" '
RW Lichota, GL Hammonds, SH Brackin, *Apps 96 pp 117–128*

An automated tool from **054409** and **054444** for the modelling and analysis of cryptographic protocols is described. It incorporates a CASE tool for protocol modelling, which is then translated into a HOL implemented variant of the GNY logic.

061426 'Threat Scenario as a Means to Formally Develop Secure Systems'
V Lotz, *ESORICS 96 pp 242–265*

The author proposes a new method to develop systems that satisfy application specific security requirements, which are defined as a result of threat identification and risk analysis. It can cope with those application level threats whose effects can be expressed in the language of timed streams (e.g., an attacker can insert at most one bogus message between two genuine ones).

061427 'A Joint Authorisation Scheme'
MR Low, JA Malcolm, *Operating Systems Review v 31 no 1 (Jan 97) pp 88–96*

The authors show that the self authenticating proxies of Low and Christianson (**034216**) can be used to implement many of the requirements of joint authorisation proposed by Varadharajan and Allen (**061248**). They also show that the syntax of

joint authorisation can be quite complex; in addition to having two signatories on a corporate cheque, we can have situations where a single individual has to present two separate forms of ID, and further complications relating to delegation, roles, and guarantees. The self-authenticating proxy mechanism allows these situations to be handled precisely.

061428 'Modelling a Public-Key Infrastructure'
U Maurer, *ESORICS 96 pp 325–349*

This article presents both deterministic and probabilistic models of trust in certification structures. In the latter, trust is increased by using independent certification paths.

061429 'Lightweight Micro-cash for the Internet'
W Mao, *ESORICS 96 pp 15–32*

The author proposes a microcash technique based on a one time signature scheme derived from Schnorr's signature. He describes protocols for cash withdrawals, payment and deposit for both fixed and subdivisible value coins. The double spending problem is solved by enabling the bank to compute the double spender's private key, and thus revoke the corresponding public key.

061430 'On Cryptographic Techniques for On-line Bankcard Payment Transactions Using Open Networks'
W Mao, *Protocols 96 pp 1–17*

A critical review of the STT and SEPP specifications for bankcard payments over open networks is provided. Various problems are identified, with possible misuse and/or overengineering of security services. Solutions to the problems are proposed.

061431 'Cryptography and the Internet: Lessons and Challenges'
K McCurley, *Asiacrypt 96 pp 50–56*

The author describes the current effort to incorporate protective measures into the Internet protocol suite and discusses the engineering lessons learned. Like the introduction of radio, the growth of the Internet will bring about a sea change in cryptography, with issues including automated rather than manual operation, very large scale, difficulties of secure naming, middleperson attacks, the need to offer protection at multiple layers, growing complexity, commercial considerations, escrow, and service denial attacks.

061432 'Analyzing the Needham-Schroeder Public Key Protocol: A Comparison of Two Approaches'
CA Meadows, *ESORICS 96 pp 351–364*

This article compares the NRL Protocol Analyzer and the model checker FDR; the latter found an attack on the Needham-Schroeder public key protocol) (**044430**), which the NRL tool also detected as the test case; it also detected several new attacks that work if names and nonces can be confused. It concludes that the two tools are to a certain extent complementary.

061433 'Efficient Certificate Revocation'
S Micali, *RSA 97*

The author discusses the performance aspects of various possible approaches to managing certificate revocation lists and suggests various ways of compressing the data they contain, including confirmation lists and differential revocation of various kinds.

061434 'Privacy and Authentication Protocols for PCS'
S Mohan, *IEEE Personal Communications v 3 no 5 (Oct 96) pp 34–38*

The author describes the two authentication protocols expected to be incorporated into PCS Interim Standard 41 by EIA/TIA: the first holds the user's long term secret at the home location, while the second forwards it to the visited location. A performance

analysis shows that (security issues apart) the former is better for a more mobile population, and the latter for a more stable one.

061435 'Cost-Effective Payment Schemes with Privacy Regulation'
D M'Raïhi, *Asiacrypt 96 pp 266–275*

A fair electronic payment scheme is proposed, in which trustees blind coins to escrow users' identities and users may trade computational effort for linkability of payments.

061436 'On the design of security protocols for mobile communications'
Y Mu, V Varadharajan, *ACISP 96 pp 134–145*

This paper tackles the design of authentication and key distribution protocols for a mobile computing environment. It reviews security issues in such environments and analyses a set of protocols proposed by Beller et al, as well as modifications proposed by Carlson. It points out some weaknesses and suggests improvements. It also suggests ways of providing anonymity for users of such systems. Finally, it considers end-to-end security and proposes a protocol for mutual authentication and key establishment between mobile users.

061437 'Electronic Payments of Small Amounts'
TP Pedersen, *Protocols 96 pp 59–68*

The author describes a system for electronic payments composed of more payments of small amounts in real-time. These 'tick payments' are applicable for phones, metering services, etc. The scheme can be applied both on-line and off-line, and employs recursive hashing to chain single payments. The main advantage is in reducing the requirements for computation and communication.

061438 'Object Oriented Cryptographic Facility Design: Export Considerations'
J Press, *Computers and Security v 15 no 6 (1996) pp 507–514*

The author describes ICL's cryptographic architecture and discusses some interesting questions of protocol design that it raised. It has a hierarchy of object classes ranging from managed objects at the top down through policy mechanisms to algorithm objects at the bottom, and a big problem was to protect the linking mechanism so that algorithms could not be replaced by users — whether these were attackers trying to replace strong crypto with weak, or purchasers of 'export' versions trying to do the reverse. The solution is to have separate crypto support facilities for the infrastructure (where the crypto is always strong) and for user data (where it may not be). He goes on to discuss mechanisms for handling multiple algorithms and key escrow.

061439 'Proxies for Anonymous Routing'
MG Reed, PF Syverson, DM Goldschlag, *Apps 96 pp 95–104*

This article provides more information on the authors' 'onion routing' infrastructure (see **054421**) whose goal is to protect the US Navy's TCP/IP communication against traffic analysis. Details include how one goes about padding messages and destroying the anonymous connection after use. Onion routing has been implemented for HTTP, rlogin, SMTP and FTP.

061450 'Plugging the Holes in Host-based Authentication'
J Reid, *Computers and Security v 15 no 8 (1996) pp 661–671*

This article discusses a number of ways of attacking Internet protocols and reviews the strengths and weaknesses of IPSEC, SSL and SSH. It also discusses whether a future secure DNS would win out over the proposed X.509 hierarchy as a global trust backbone.

061451 'PayWord and MicroMint: Two Simple Micropayment Schemes'
RL Rivest, A Shamir, *Protocols 96 pp 69–87*

The authors present two micro-payment schemes for purchases over open networks. Both schemes are efficient, but require additional measures to counter large-scale fraud. The first scheme uses chains of hash values with a signed root. The second scheme is based on k-way hash function collisions as coins, where the basic point is that the computation of coins is economic on a large scale only. The former scheme is ideal for many payments to a single merchant, while the latter is good for many small payments to many merchants.

061452 'The PGP Moose — Implementation and Experience'
G Rose, *LISA 96 pp 155–160*

PGP Moose is free software designed to monitor the news postings of newsgroup moderators and automatically cancel forged messages. This article describes the protocol, its history, and early operating experience.

061453 'Multisignature Algorithms for ISO 9796'
S Russell, *ACM SIGSAC Review v 15 no 1 (Jan 97) pp 11–14*

This presents two possible adaptations of ISO 9796 to cope with multisignatures.

061454 'CSP and Anonymity'
S Schneider, A Sidiropoulos, *ESORICS 96 pp 198–218*

The article defines formally the property of anonymity with respect to different contexts using the CSP notation. It focusses on the interactions between system components. The approach is then applied, using the FDR model-checking tool, to a machine-assisted analysis of the dining cryptographers problem and some variants. From these examples, it emerges that CSP analysis provides useful feedback about which particular property of a system violates the anonymity requirement.

061455 'Automatic Event-Stream Notarization Using Digital Signatures'
B Schneier, J Kelsey, *Protocols 96 pp 155–169*

The idea of padding hashed messages with auditing information to form a block of the length required by a signature mechanism is discussed. The presented signature packet format includes token and key IDs, sequence number, values for chaining hashes of signed and received packets, and so on. This way the token embeds hard-to-tamper auditing information and allows for the construction of robust token-based protocols.

061456 'Distributed Proctoring'
B Schneier, J Kelsey, J Walker, *ESORICS 96 pp 172–182*

The article presents a protocol for distributed proctoring. which allows a network of test graders to grade individual problems solved by a network of test takers. Mutual anonymity of the test takers and graders is ensured by trusted anonymous intermediary communication nodes. Audit trails are kept in case of grading disputes.

061457 'Subliminal Channels: Some Recent Developments'
GJ Simmons, *RSA 97*

The author refines his conjecture about subliminal channel bandwidth in the light of the Newton Channel (**061602**) and discusses how to deal with the 'balking channel' introduced in **054604**: the bandwidth of this can be reduced by getting the signer to utter more than one signature and forwarding a randomly chosen subset of them, but it can never be eliminated. For example, a 'sleeper' under deep cover in a foreign country might wait for decades for a one-bit wake-up signal before carrying out his mission, and the only way for a censor to be sure that this signal will not get through is to forward no messages at all.

061458 'Credits and debits on the Internet'
MA Sirbu, *IEEE Spectrum v 34 no 2 (Feb 97) pp 23–29*

The author describes a number of electronic payment protocols including CyberCash, SET and NetBill.

061459 'Code acquisition scheme for frequency hopping radio in channels with fading'
BM Todorović, *Electronics Letters v 33 no 3 (30/1/97) pp 177–179*

Key management is tricky in low-probability-of-intercept systems, and particularly when a fading channel forces frequent resynchronisation. This paper presents a 3-level scheme to enable frequency hop radios to resynchronise rapidly and calculates the probabilities of false alarm, false lock and false dismissal.

061460 'Digital IDs'
J Udell, *Byte (Mar 97) pp 115–118*

This article describes how certificates work with SSL, and a number of tools on offer to help develop and test CA facilities. It discusses the policy issue of whether companies such as magazine publishers should certify their subscribers, and some of the compatibility problems arising between different types of certificate.

061461 'On the Design of Secure Electronic Payment Schemes for Internet'
V Varadharajan, Y Mu, *Apps 96 pp 78–87*

Secure credit card based payment schemes are discussed from the perspectives of relying on a merchant's honesty and the client's need to store her own private key securely. A new payment protocol introduces a pseudo-secret key computed as a hash of xored values of PIN, card number and a freshly generated Electronic Commerce ID. The latter serves as an additional password for the user and also for identifying Internet based transactions.

061462 'Public Key Infrastructure'
E Verheul, BJ Koops, H van Tilborg, *Computer Law and Security Report v 13 no 1 (Jan/Feb 97) pp 3–14*

Having reviewed the problems with existing key escrow proposals, the authors suggest an alternative: the session key of a message is encrypted under the public keys of both the recipient and the escrow agent. Supplementary binding information proves that both these packets contain the same session key, without giving any information about its value.

061463 'Formal Semantics for Authentication Logics'
G Wedel, V Kessler, *ESORICS 96 pp 219–241*

The authors present a new BAN-like logic, that includes negation, for the analysis of authentication protocols. They provide a formal semantics in order to prove its soundness, and use it to verify a protocol proposed by ETRI for the UMTS system.

061464 'Transactions Using Bets'
D Wheeler, *Protocols 96 pp 89–92*

An innovative way of arranging small cash (either physical or electronic) payments through zero average loss betting is outlined: to pay 63c with a $1 bill, one simply gambles with the merchant with appropriate odds. This would reduce exchange and transfer costs, though it would also require changes not only to schemes' design, but also to some of their underlying principles.

061465 'Sleepy Network-Layer Authentication Service for IPSEC'
SF Wu, *ESORICS 96 pp 146–159*

The author presents SSGP — Sleepy Security Gateway Protocol — which offers network-layer authentication services for IPSEC. The idea is that gateways only start to authenticate when attacks are detected; to do this, the application and network layer security mechanisms cooperate.

061466 'Security Issues in an EDI Environment'
N Zhang, Q Shi, *Apps 96 pp 129–136*

The authors mention some EDI security problems and discuss non-repudiation of receipt in more detail. This leads to a new protocol, which requires a trusted third party to transfer and record the session key rather than the message itself.

061467 'Certified Electronic Mail'
J Zhou, D Gollmann, *ESORICS 96 pp 160–171*

The article discusses what are the essential requirements of a certified mail service, and presents protocols to implement them in the electronic world. Several variants of the protocol are presented, for example to prevent the recipient being selective about what messages he receives; in this case, a trusted third party gets a receipt on the mail label before forwarding the mail item itself. Other security services — such as integrity — can be easily integrated with the basic certification.

5 Secret Key Algorithms

061501 'Generating De Bruijn Sequences: An Efficient Implementation'
FS Annexstein, *IEEE Transactions on Computers v 46 no 2 (Feb 97) pp 198–200*

The author provides an $O(2^n)$ method for generating a De Bruijn sequence of order n by recursively joining up cycles.

061502 'Linearity Testing in Characteristic Two'
M Bellare, D Coppersmith, J Håstad, M Kiwi, M Sudan, *IEEE Transactions on Information Theory v 42 no 6 (Nov 96) pp 1781–1795*

The linear functions from GF(2^n) to GF(2) describe a Hadamard code of length 2^n, and the distance of a Boolean function f to a linear function, Dist(f), is thus just its distance from this code. The relationship of Dist(f) to Err(f), the rejection probability of the Blum-Luby-Rubinfeld linearity test, is studied and a nearly complete relationship between the two functions is given.

061503 'Computational experience on the distances of polynomials to irreducible polynomials'
A Bérczes, L Hajda, *Mathematics of Computation v 217 (Jan 97) pp 391–398*

The authors tabulate some 'extreme' polynomials, that is, polynomials that are at a maximum distance from irreducible polynomials.

061504 'On the Correlation Immune Functions and Their Nonlinearity'
S Chee, S Lee, D Lee, SH Sung, *Asiacrypt 96 pp 232–243*

The paper provides a discussion of the relationship between the correlation immunity and nonlinearity of the functions presented by Camion et al and discussed in **023529**. A suggestion for constructing correlation immune functions with controllable nonlinearity is outlined.

061505 'Digitals Fingerabdrücke'
H Dobbertin, *Datenschutz und Datensicherheit v 21 no 2 (Feb 97) pp 82–87*

The author surveys the MD series of hash functions, describing both the algorithms' performance and recent results in cryptanalysis. He concludes that SHA-1, RPIEMD-128 and RIPEMD-160 are to be preferred.

061506 'RIPEMD with Two-Round Compress Function is Not Collision-Free'
H Dobbertin, *Journal of Cryptology v 10 no 1 (Winter 97) pp 51–69*

If either the first or the last round of RIPEMD is omitted, the resulting hash function is not collision-free; finding collisions takes 2^{31} computations, or about a day on a 66MHz 486 PC. The methods developed to do this can also be applied to find collisions for MD4 in less than a minute.

061507 'Average equidistribution properties of compound nonlinear congruential pseudorandom numbers'
J Eichenauer-Herrman, G Larcher, *Mathematics of Computation v 217 (Jan 97) pp 363–372*

The authors establish upper, lower and average values for the discrepancies of sequences generated by computing, with respect to r distinct primes, $x(n) \equiv f_i(n) \pmod{p_i}$ where f_i is a permutation polynomial on Z_{p_i}. These turn out to be essentially the best possible, and are a good fit for the equidistribution properties of random numbers.

061508 'Correlation Attacks on Cascades of Clock Controlled Shift Registers'
W Geiselmann, D Gollmann, *Asiacrypt 96 pp 346–359*

Clock controlled shift registers may suffer from correlation attacks which exploit the fact that a zero clock input does not force a change of the register state. The

periods and linear complexity of cascades of shift registers are reviewed. Two methods to derive the correlation coefficients are used — a transformation matrix of a cascade input/output behaviour and a Markov model describing cascade state transitions.

061509 'Edit distance correlation attacks on clock controlled combiners with memory'
JD Golić, *ACISP 96 pp 169–181*

Binary keystream generators consisting of n clock-controlled shift registers combined by a function with m bits of memory are considered. The objective of the paper is to design a divide and conquer correlation attack to reconstruct the initial content of the shift register given a segment of the key stream sequence. The paper proposes a new edit distance which is the minimum number of elementary edit operations needed to transform a set of input strings to a single output string. The combinatorial problem of computing this distance is solved by using a recursive algorithm and its uses in a correlation attack on clock-controlled sequences are shown.

061510 'On period of multiplexed sequences'
JD Golić, *ACISP 96 pp 158–168*

Multiplex sequences are obtained by using one maximum-length sequence to select keystream bits from another using a multiplexer. This paper generalises such sequences by making the mapping time dependent. It turns out that the generalised multiplex sequences are describable in terms of decimated sequences. The paper uses a new result on the latter to obtain the period of the former, and finally applies this result to find the period of a class of variable-memory binary sequences introduced by Golić and Mihaljević in 1990.

061511 'Interval Algorithm for Random Number Generation'
TS Han, M Hoshi, *IEEE Transactions on Information Theory v 43 no 2 (Mar 97) pp 599–611*

The problem of generating random numbers with an arbitrary probability distribution given an arbitrary biased M-coin is solved by mapping the distribution on to intervals in [0,1) in a suitable way.

061512 'On Applying Linear Cryptanalysis to IDEA'
P Hawkes, L O'Connor, *Asiacrypt 96 pp 105–115*

The authors examine IDEA with extended sub-keys, prove that for R rounds of IDEA to be approximated at least $R + \lfloor \frac{R}{3} \rfloor$ approximations to the multiply operation are required, and argue for best approximations based on approximating the LSB in the round operations. They calculate that the probability of choosing a key with a feasible linear attack is about 2^{-100}.

061513 'Trace Representation of Legendre Sequences of Mersenne Prime Period'
JS Ho, HK Lee, HB Chung, HY Song, KC Yang, *IEEE Transactions on Information Theory v 42 no 6 (Nov 96) pp 2254–2255*

If $p = 2^n - 1$ is prime, then Legendre sequences of period p can be represented explicitly by the trace function on GF(2^n).

061514 'On the limit of maximal density of sequences with a Perfect Linear Complexity Profile'
AED Houston, *Designs, Codes and Cryptography v 10 no 3 (Mar 97) pp 351–359*

A binary sequence has a perfect linear complexity profile if all the jumps in its linear complexity have height exactly 1. It is proved that as the length of such a sequence tends to infinity, the proportion of 1's over all sequences of a given length tends to 2/3.

061515 'On the Design of a Stream Cipher and a Hash Function Suitable to Smart Card Applications'
Y Kim, S Lee, C Park, *Cardis 96 pp 1–10*

The authors apply results from Krawczyk's 'Toeplitz hashing' in **034520** to design algorithms for smart card applications. They extend the linear feedback shift register scheme over GF(2) to GF(2^8) for a hash function and present a stream cipher based on two shift registers.

061516 'Hash Functions Based on Block Ciphers and Quaternary Codes'
L Knudsen, B Preneel, *Asiacrypt 96 pp 77–90*

Constructions of hash functions based on m-bit block ciphers are reviewed and a new attack on LOKI-DBH mode is presented (it can find collisions in $2^{3m/4}$ encryptions). A new hash function construction is given, based on quaternary codes, for which collision finding should take more than 2^m encryptions. This method supports functions at a higher security level than existing proposals, given the same computational efficiency; however more internal memory is needed. It is secure so long as the underlying elementary hash function is.

061517 'Chaotic bit sequences for stream cipher cryptography and their correlation function'
T Kohda, A Tsuneda, *Proceedings of the SPIE (The International Society for Optical Engineering) v 2612 pp 86–97*

This paper presents a stream cipher system whose running key sequences are threshold and bit sequences generated by Chebyshev polynomials. It has some good characteristics: in particular, it can generate independent identically distributed binary random variables, and their correlation properties are at least as good as those of standard ciphers.

061518 'Statistics of Chaotic Binary Sequences'
T Kohda, A Tsuneda, *IEEE Transactions on Computers v 46 no 1 (Jan 97) pp 104–112*

The authors present a sufficient condition for a class of chaotic sequences to produce a sequence of independent identically distributed binary random variables.

061519 'Generalization of Higher Order SAC to Vector Output Boolean Functions'
K Kurosawa, T Satoh, *Asiacrypt 96 pp 218–231*

The paper studies an extension of the k-order strict avalanche criterion to vector output Boolean functions — $n \times m$ S-boxes — called (n, m, k)-SAC functions. The purpose is to investigate the security of block ciphers against general attacks that keep some input bits constant. Bounds on k and m are given, which imply bounds on the structure of effective S-boxes.

061520 'A Strength Evaluation of the Data Encryption Standard'
K Kusuda, T Matsumoto, *ISO TC 68 WG 7 subcommittee 2*

This technical report reviews all the published attacks on DES, including linear and differential analysis and various possible keysearch machines. Statistical and group theoretic properties are also covered, as is triple DES, which they consider to be very secure until 2020 or 2050 depending on what kind of time-memory tradeoffs are available.

061521 'Conditional Correlation Attack on Nonlinear Filter Generators'
S Lee, S Chee, S Park S Park, *Asiacrypt 96 pp 360–367*

The concept of a conditional linear approximation for the filter function is introduced, leading to a conditional correlation attack which enables the conditional correlation attack from **044502** and **052516** to be improved. An attack that is effective against most nonlinear filter generators is described.

061522 'Optimal PN Sequence Design for Quasisynchronous CDMA Communication Systems'
XD Lin, KH Chung, *IEEE Transactions on Communications v 45 no 2 (Feb 97) pp 221–226*

When spread-spectrum systems have synchronisation errors of at most one bit, preferentially-phased Gold codes are optimal for the spreading sequence. In this paper, the authors show that when several chips of error may occur, one can improve performance by using the more numerous generalised GMW sequences.

061523 'Controlling chaos in random Boolean networks'
B Luque, RV Solé, *Europhysics Letters v 37 no 9 (97) pp 597–602*

The authors studied 'random Boolean networks', pseudorandom generators in which automata, that compute randomly chosen Boolean functions on k variables, are each connected to k others and run from a randomly chosen initial state. They found that for $k > 2$, the behaviour generally appears to be chaotic, but it can be controlled to some extent by setting a subset of the machine's state to some fixed value every so many steps. Some analytic results about such systems are given.

061524 'A faster cryptanalysis of the self-shrinking generator'
M Mihaljević, *ACISP 96 pp 182–189*

The author presents an attack on the self shrinking generator (**032529**). It assumes that the characteristic polynomial of the shift register is known, and uses the output sequence for hypothesis testing and reducing, probabilistically, the set of hypotheses about the initial state. The attack is compared to the other known attacks and is shown to be superior to them in the majority of cases.

061525 'Generalized Feistel Networks'
K Nyberg, *Asiacrypt 96 pp 91–104*

The security of Feistel networks without auxiliary permutations in the round function is discussed, both for resistance against differential and linear cryptanalysis. Upper bounds for a generalised Feistel network of up to 4 S-boxes in parallel per round are derived.

061526 'Secure Communication with Chaotic Systems of Difference Equations'
S Padadimitriou, A Bezirianos, T Bountis, *IEEE Transactions on Computers v 46 no 1 (Jan 97) pp 27–38*

The authors present keystream generators that produce 'chaotic' output by combining piecewise linear functions, trigonometric functions, and modular reduction.

061527 'Improving bounds for the number of correlation immune Boolean functions'
SM Park, SJ Lee, SH Sung, KJ Kim, *Information Processing Letters v 61 no 4 (28/2/97) pp 209–212*

By constructing correlation immune Boolean functions recursively, the authors derive tighter upper and lower bounds on their numbers.

061528 'François Viète, father of modern cryptanalysis — two new manuscripts'
P Pesic, *Cryptologia v XXI no 1 (Jan 97) pp 1–29*

Two recently discovered manuscripts show that François Viète, widely regarded as the father of modern algebra, can also be considered the father of systematic cryptanalysis. He used frequency analysis, including digraphs and trigraphs, to distinguish vowels from consonants and to test various hypotheses; he was confident of being able to solve arbitrary nomenclators. His work was done on behalf of France against Spanish and Italian traffic; his confidence in his method enabled decrypts to be published as part of court intrigues. English translations of the manuscripts are given.

061529 'Cryptography based on transcendental numbers'
J Pieprzyk, H Ghodosi, C Charnes, R Safavi-Naini, *ACISP 96 pp 96–107*

The aim of this paper is to show how floating point arithmetic can be used as the basis of cryptographic algorithms. One of their ideas is to encrypt m as $c = (m + a)^b$ where a and b are quadratic irrationals. This means that c is transcendental by Baker's theorem, and it can be shown that irrationals pass the next bit test. Some analysis of computational effort is given.

061530 'Want to encrypt data?'
B Rothke, *Datamation (Mar 97) pp 122–124*

An accountant recommends that the replacement for DES should be triple DES on the grounds that it is thoroughly tested, widely implemented and most likely to protect existing security investments.

061531 'A New Universal Test for Bit Strings'
B Sadeghiyan, J Mohajeri, *ACISP 96 pp 311–319*

A new test for both local and overall randomness of bit strings is suggested. It is based on the next-bit test model, evaluating the success with which an attacker can predict the next bit of a string, and can be applied to a string of any length.

061532 'Boolean Functions Classification via Fixed Polarity Reed-Muller Forms'
CC Tsai, M Marek-Sadowska, *IEEE Transactions on Computers v 46 no 2 (Feb 97) pp 173–186*

The authors present a way to characterise Boolean functions using a number of properties such as linearity, symmetry and self-duality; it identifies functions that are equivalent up to input permutation, input negation or output negation.

061533 'On a method of cryptanalysis for cryptosystem with involution'
Y Tsunoo, E Okamoto, T Uematsu, *Electronics and Communications in Japan Part 3 v 78 no 5 pp 1-11*

A new cryptanalytic method for involution-type cryptosystems is presented and it is shown by example that it can be applied practically in a ciphertext-only attack on the one-way function MAP. This is a journal version of the work reported in **031525** and **034546**.

061534 'Linear complexity profiles and jump complexity'
MZ Wang, *Information Processing Letters v 61 no 3 (14/2/97) pp 165–168*

The author extends Rueppel's work on complexity profiles to calculate the expected number of jumps in the profile and its variance. The resulting randomness test easily detects that sequences such as that described in **022527** are not pseudorandom.

061535 'On construction of resilient functions'
CK Wu, E Dawson, *ACISP 96 pp 79–86*

An (n, m, t) resilient function takes binary n-tuple inputs and produces binary m-tuple outputs such that if any t bits of the input are fixed and the remaining $n - t$ positions vary over all possible values, every output m-tuple occurs with the same frequency. They could be important in the design of cryptographic components such as s-boxes. This paper reviews known results in the field and underlines the difficulty of constructing non-linear resilient functions — a significant unsolved problem. Finally, it suggests a method of constructing infinite classes of resilient functions from smaller ones using error correcting codes.

061536 'Cryptanalysis of "nonlinear-parity circuits" proposed at Crypto 90'
AM Youssef, SE Tavares, *Electronics Letters v 33 no 7 (27/3/97) pp 585–586*

The authors show that a Boolean function proposed at Crypto 90 by Koyama and Terada for use in block ciphers is actually affine.

6 Public Key Algorithms

061601 'How to Date Blind Signatures'
M Abe, E Fujisaki, *Asiacrypt 96 pp 244–251*

The authors present an RSA-based blind signature scheme where signatures include information common to both sender and signer. To preserve perfect confidentiality, the common information is incorporated into the public key rather than being part of the message. Forging these partially-blind signatures remains as difficult as breaking RSA.

061602 'Minding your p's and q's'
R Anderson, S Vaudenay, *Asiacrypt 96 pp 26–35*

The authors survey a number of attacks based on unwise choices of the parameters of discrete log based public key cryptosystems, and present some new attacks as well. Many of these involve the choice of a generator g whose order is not prime; others involve malicious choices of message key, and/or an interaction between the message key and the public parameters. The US Digital Signature Standard appears to have taken some (but not all) of these attacks into account: it is described as 'ElGamal with most of the bugs fixed'. There are also attacks on some systems that combine knapsacks with discrete log.

061603 'Server-Supported Signatures'
N Asokan, G Tsudik, M Waidner, *ESORICS 96 pp 131–143*

The authors propose a fair non-repudiation technique based on hash chaining. A signature server generates non-repudiation tokens on behalf of the users; at the user's request, it will generate a signature on a message and an integer i, which the user then authenticates by producing the i-th preimage of the root of a hash chain. Protocols for non-repudiation of origin and receipt are presented. Storage requirements, robustness and the revocation of hash chains are also discussed in detail.

061604 'Cryptographic Protocols Based on Real-Quadratic A-Fields'
I Biehl, B Meyer, C Thiel, *Asiacrypt 96 pp 15–25*

The authors define the Distance, Discrete-Logarithm and Diffie-Hellman problems in the cycle of reduced principal ideals in real-quadratic A-fields. Their difficulty and the relationship between them are discussed, and a computationally difficult problem of computing square roots of reduced principal ideals in real-quadratic A-fields is introduced. A simple crypto protocol based on this problem, and another based on Diffie Hellman, are presented.

061605 'On the Efficiency of One-Time Digital Signatures'
D Bleichenbacher, U Maurer, *Asiacrypt 96 pp 145–158*

Digital signature schemes based on a general one-way hash function are discussed, and characterised by means of directed acyclic graphs. Several constructions of one-time signature schemes are analysed and efficiency results derived. It is argued that they can be more efficient than schemes based on trapdoor one-way functions, and also give more freedom for the choice of the underlying cryptographic function.

061606 'Efficient and Secure Conference-Key Distribution'
M Burmester, YG Desmedt, *Protocols 96 pp 119–129*

An improvement on the authors' conference key distribution scheme from **032605** is given. The new scheme based on the Diffie-Hellman key exchange as a cryptographic primitive is more effective — the cost per user is about 1.5 times that of the primitive. Also, there are no restrictions on the specific network or the cryptographic primitive.

061607 'Mis-representation of Identities in E-cash Schemes and how to Prevent it'
A Chan, Y Frankel, P MacKenzie, Y Tsiounis, *Asiacrypt 96 pp 276–285*

An attack on Brands' e-cash scheme is presented, allowing a malicious user to double-spend without incurring detection. A workaround is proposed.

061608 'A digital signature scheme based on the theory of quadratic residues'
CC Chang, JK Jan, HC Kowng, *Cryptologia v XXI no 1 (Jan 97) pp 55–70*

The authors propose a signature scheme in which non-repudiation is added to a symmetric authentication protocol by means of a Rabin signature on a hash of the message and a value from a hash chain.

061609 'The Cryptographic Security of the Syndrome Decoding Problem for Rank Distance Codes'
F Chabaud, J Stern, *Asiacrypt 96 pp 368–381*

The authors present an algorithm for syndrome decoding of a (n,k,r) rank distance code over (2^m) with complexity $O((nr+m)^3 q^{(m-r)(r-1)})$ and thus show that the choice of parameters in the identification schemes like in **034608** should be re-considered.

061610 'Efficient and Provable Security Amplifications'
R Cramer, I Damgård, T Pedersen, *Protocols 96 pp 101–109*

The paper shows a new transformation of signature schemes secure against known message attacks into schemes secure against adaptively chosen message attacks. The complexity of the derived scheme should be only double that of the original scheme. The amplification is also applied to block encryption schemes for converting systems secure against known plaintext attacks to systems secure against chosen plaintext attacks. the technique is more efficient than that of Even, Goldreich and Micali for signatures, but not for block encryption.

061611 'A Comparison of RSA and the Naccache-Stern Public-Key Cryptosystem'
TW Cusick, *Protocols 96 pp 111–116*

The author reviews the differences between the new public key system of Naccache-Stern and RSA. He concludes that RSA is superior in various implementation details (public key length, decryption time and encipherment message expansion), whereas the Naccache-Stern system has faster encryption and appears to be not susceptible to factoring complexity challenges.

061612 'On Schnorr's Preprocessing for Digital Signature Schemes'
P de Rooij, *Journal of Cryptology v 10 no 1 (Winter 97) pp 1–16*

At Eurocrypt 91, the author showed an attack on a preprocessing scheme that had been proposed along with the Schnorr signature scheme; it involved replacing the computation of the random session key with a linear combination of precomputed secrets. Schnorr then proposed a more complicated preprocessing scheme; the attack is adapted to it in this article.

061613 'Fälschungssicherheit digitaler Signaturen'
D Fox, *Datenschutz und Datensicherheit v 21 no 2 (Feb 97) pp 69–74*

The author reviews the various known attacks on RSA and DSA signature mechanisms, briefly describes various provable secure and optimised schemes, and discusses likely attacks on implementations including existential forgery of RSA signatures and implementation failures.

061614 ' "Indirect Discourse Proofs": Achieving Efficient Fair Off-Line E-cash'
Y Frankel, Y Tsiounis, M Yung, *Asiacrypt 96 pp 286–300*

The authors propose a fair off-line e-cash scheme, based on the Brands scheme and on the notion of indirect discourse proofs, which allow users to prove that a third party possesses a certain future capability (such as the ability of trustees to trace coins). The scheme is off-line from the trustees for withdrawal, payment and deposit; off-line from the bank for payment; and provides for both owner and coin tracing. Otherwise, its security and efficiency do not depart significantly from Brands' scheme.

061615 'Practical Escrow Cash Systems'
E Fujisaki, T Okamoto, *Protocols 96 pp 33–48*

The paper introduces two examples of an 'escrow cash scheme' protecting user's privacy unless a number of trustees collaborate to identify him. The RSA signature scheme is used in the former function and an arbitrary scheme in the latter. Any signature scheme can be specified for the customer and any blind signature scheme for the bank.

061616 'Cryptosystems for Hierarchical Groups'
H Ghodosi, J Pieprzyk, C Charnes, R Safavi-Naini, *ACISP 96 pp 275–286*

Two cryptosystems are presented, one based on the ElGamal scheme and the other on RSA. The former has a weakness in that higher levels can impose lower levels to retrieve a false message; this cannot happen with the latter scheme. In these top-down hierarchical schemes, participants on higher levels have to perform crypto-operations before the lower level participants do. In both schemes a trusted dealer sets up the system choosing keys, determining and distributing secret shares, etc. Two types of shares are used — static shares for computing partial results, and dynamic shares for controlling information flow from one level to another.

061617 'Digital signature for Diffie-Hellman public keys without using a one-way function'
L Harn, *Electronics Letters v 33 no 2 (16/1/97) pp 125–126*

The author proposes four ElGamal variants which he claims do not require the message to be hashed before signature.

061618 'Protocol Failures for RSA-Like Functions Using Lucas Sequences and Elliptic Curves'
M Joye, JJ Quisquater, *Protocols 96 pp 93–100*

The authors extend an attack with related plaintexts and small public exponents to the RSA like cryptosystems proposed by Demytko (**023609**), KMOV and LUC (**024620**) systems, of which the first two are elliptic curve variants of RSA and the third based on Dickson polynomials. This generalises the attack by Coppersmith et al on classical RSA (**053606**).

061619 'Elliptic Curves and Cryptography'
A Jurišić, AJ Menezes, *Dr Dobbs Journal (Apr 97) pp 26–36*

The authors provide a gentle introduction to elliptic curve cryptosystems, describe a draft standard elliptic analogue of the digital signature algorithm, and discuss its relative security.

061620 'A Chosen Message Attack on Demytko's Elliptic Curve Cryptosystem'
BS Kaliski, *Journal of Cryptology v 10 no 1 (Winter 97) pp 71–72*

The Demytko cryptosystem **023609** was claimed superior to RSA because of resistance to low exponent attacks and to signature forgery under chosen message attack. The former claim was shown to be invalid in **034625** and the latter in this article.

061621 'IEEE P1363: A Standard for RSA, Diffie-Hellman, and Elliptic-Curve Cryptography (Abstract)'
BS Kaliski Jr., *Protocols 96 pp 117–118*

The author gives a very brief description of this standard; Internet pointers are provided.

061622 'Convertible Group Signatures'
SJ Kim, SJ Park, DH Won, *Asiacrypt 96 pp 311–321*

The authors review an extension to group signatures — convertible group signatures — which allow the signer to turn his group signatures into ordinary signatures by release of a bit string, and present two schemes of this kind (but see **061624**).

061623 'Generating Standard DSA Signatures Without Long Inversion'
AK Lenstra, *Asiacrypt 96 pp 57–64*

The computational cost of modular arithmetic in DSA is discussed: inversion is particularly expensive for memory-bound applications. A new method is presented that simultaneously generates k and k^{-1}. The method does not provide a truly random value of k but its unpredictability is analysed closely, and a comparative analysis is presented of implementation results.

061624 'Directed Signatures and Application to Threshold Cryptosystems'
CH Lim, PJ Lee, *Protocols 96 pp 131–138*

The authors review the concept of directed (designated receiver) signatures presented also in **021623** and similar to the designated confirmer signatures introduced in **034631**. These signatures should be verifiable only with the participation of a designated signature receiver. A scheme based on Schnorr's signatures is given, and is also presented in a threshold variation.

061625 'Remarks on convertible group signatures of Asiacrypt 96'
CH Lim, PJ Lee, *Electronics Letters v 33 no 5 (27/2/97) pp 383–384*

A scheme of Kim et al presented at Asiacrypt 96 (**061622**) is vulnerable to an attack of complexity 2^{37}; in addition, users can hide their identities by generating their secret keys randomly. This also makes it impossible for users to convert their group signatures into normal ones. However, it is suggested that the scheme might be recycled for anonymous signature applications.

061626 'A Group-Oriented (t,n) Undeniable Signature Scheme Without Trusted Center'
CH Lin, CT Wang, CC Chang, *ACISP 96 pp 266–274*

A general (t, n) undeniable group signature scheme is presented, extending **021614** using a polynomial function of degree $t-1$. Each member possesses an individual secret key; the group public key is created by all the members cooperating. Any t members can sign a message or assist a verifier in checking the signature. No trusted centre is required for the scheme, although the selection of parameters has to be done a reliable way.

061627 'How to Utilize the Transformability of Digital Signatures for Solving the Oracle Problem'
M Mambo, K Sakurai, E Okamoto, *Asiacrypt 96 pp 322–333*

Transformable signatures can be applied to solving the oracle problem of a blind decoding scheme based on ElGamal. The proposed protocol keeps decrypted messages untraceable and shows a possible use of the otherwise unfavourable transformability feature. The relevance of transformable signatures to blind signature, divertible zero-knowledge interactive proof and some variants of the ElGamal signature, is discussed.

061628 'On the Risk of Disruption in Several Multiparty Signature Schemes'
M Michels, P Horster, *Asiacrypt 96 pp 334–345*

A universal forgery attack against several multisignature schemes (e.g., **032613**, **044611**) is presented. This type of attack comes from an insider (in some schemes also colluding with the passive clerk), who has received some values from co-signers. Other problems with some of the schemes (and also with schemes from **032617**) are mentioned and a suggestion for fixes is briefly outlined.

061629 'GOST 34.10 — a brief overview of Russia's DSA'
M Michels, D Naccache, H Petersen, *Computers and Security v 15 no 8 (1996) pp 725–732*

The Russian answer to DSA is a similar algorithm but with the signature calculated by $s = xr + kh(M) \pmod q$ rather than $s = (h(M) = xr)/k \pmod q$; the prime q is at least 254 bits long. Signature generation is 1.6 times slower than with DSA, while verification is twice as fast (and can be speeded up further by nonstandard techniques). It is used with a hash function, GOST 34.11, that is derived from the partially classified GOST 28147 block cipher.

061630 'A Message Recovery Signature Scheme Equivalent to DSA over Elliptic Curves'
A Miyaji, *Asiacrypt 96 pp 1–14*

Some issues with the ElGamal signature and its variants — DSA and the message recovery scheme from **051609** — are reviewed, together with the concept of equivalent classes and strong equivalences. It is explained why ElGamal is not strongly equivalent to DSA and thus why the attack of Bleichenbacher from **053602** works only for ElGamal. Aspects of ElGamal-based signature schemes over elliptic curves are then reviewed: those elliptic curve signature schemes that are vulnerable to a variant of the Bleichenbacher attack are characterised, and a means of stopping the attack is described.

061631 'Fast digital signature scheme based on the quadratic residue problem'
DH Nyang, JS Sang, *Electronics Letters v 33 no 3 (30/1/97) pp 205–206*

The authors propose a variant on Rabin signatures: for signature s and message m, $s^4 \equiv m^2 B$ modulo n, where B is either 1 or a suitable constant that depends on the quadratic residuosity of the message and is chosen to simplify signature generation.

061632 'Provably Secure Blind Signature Schemes'
D Pointcheval, J Stern, *Asiacrypt 96 pp 252–265*

In the context of blind signatures, many previous definitions of security for signature schemes are no longer applicable. A definition is therefore proposed: blind signatures should prove resilient to 'one-more forgery' where a user, after obtaining ℓ blind signatures from the signer, is able to create $\ell + 1$ signatures. A class of blind signature schemes, based on witness-indistinguishable adaptation of identification protocols, is then proven secure in the random oracle model with respect to this type of attack.

06633 'A New Paradigm for Public Key Identification'
J Stern, *IEEE Transactions on Information Theory v 42 no 6 (Nov 96) pp 1757–1768*

In this journal version of **024622**, the author describes how to use syndrome decoding for zero-knowledge identification. He suggests two identity based variants of the scheme as topics for further research.

061634 'Conference key distribution system with user anonymity based on algebraic approach'
TC Wu, *IEE Proceedings on Computers and Digital Techniques v 144 no 2 (Mar 97) pp 145–148*

The author presents a conference key scheme that combines Diffie Hellman with matrix algebra.

061635 'Cryptanalysis and repair of the multi-verifier signature with verifier specification'
SM Yen, *Computers and Security v 15 no 6 (1996) pp 537–544*

Three flaws are found in a multiple-specified-verifier scheme of Laih and Yen: one of the verifiers might cheat by inserting random data and thus cause the verification to fail, and there are two conspiracy attacks which cause the signature to be accepted initially by the group but to subsequently fail in court. Some partial countermeasures are suggested.

7 Computational Number Theory

061701 'A World Wide Number Field Sieve Factoring Record: On to 512 Bits'
J Cowie, B Dodson, RM Elkenbracht-Huizing, AK Lenstra, PL Montgomery, J Zayer, *Asiacrypt 96 pp 382–394*

The authors describe their world record factorisation of RSA130 in April 96. The paper establishes that 130 digits is well past the crossover point at which the Number Field Sieve becomes superior to the Quadratic Sieve. The sieving and matrix steps are discussed; it is estimated that the sieving step for the NFS factorisation of a 512 bit RSA modulus would require about thirty times more effort than the RSA130 work. Also, the WWW interface to the sieving program is described.

061702 'A Fast Software Implementation for Arithmetic Operations in $GF(2^n)$'
E De Win, A Bosselaers, S Vandenberghe, P De Gersem, J Vandewalle, *Asiacrypt 96 pp 65–76*

The authors present a software implementation of arithmetic operations in finite fields of characteristic two; it treats field elements as polynomials with coefficients in $GF(2^{16})$, and is optimised for the implementation of elliptic curve cryptosystems. Precalculated lookup tables are also used. The field operations in the new representation are described and a comparison with standard basis arithmetic is given.

061703 'Parallel Distinct Degree Factorisation Algorithm'
T Fujise, H Murao, *ISSAC 96 pp 18–25*

The authors present an algorithm to obtain the distinct degree factorisation of a given polynomial of degree n within time almost $O(n^2)$ using $\sqrt{n}$ processors and $n^{3/2}$ storage.

061704 'Factoring Polynomials Using Binary Representations of Finite Fields'
J Ganz, *IEEE Transactions on Information Theory v 43 no 1 (Jan 97) pp 141–153*

A new efficient algorithm for factoring polynomials in fields of large characteristic is obtained by combining Berlekamp's trace method with a suitable binary representation. This finally gives a proof that polynomial factoring is easy in every finite field.

061705 'Note on shortest and nearest lattice vectors'
M Henk, *Information Processing Letters v 61 no 4 (28/2/97) pp 183–188*

The author shows that the shortest lattice vector problem is polynomial time equivalent to the nearest lattice vector problem.

061706 'Improvements on the accelerated integer GCD algorithm'
MS Sedjelmaci, C Lavault, *Information Processing Letters v 61 no 1 (14/1/97) pp 31–36*

Sorensen's fast k-ary reduction GCD algorithm is shown to have a worst case number of iterations $\frac{1}{2}\lfloor \log_\phi(k) \rfloor$ where $\phi = \frac{1}{2}(1+\sqrt{5})$.

061707 'Arithmetic and Factorization of Polynomials over $\mathbf{F}_2$'
J von zur Gathen, J Gerhard, *ISSAC 96 pp 1–9*

The authors survey modern algorithms for factoring polynomials over GF(2) and describe a number of optimisations, especially for distinct degree factorisation. By using these, they developed a system that factors up to degree about 100,000 in a day on two workstations. They report on the performance gain from various optimisations as a function of the degree.

061708 'Factoring Modular Polynomials'
J von zur Gathen, S Hartlieb, *ISSAC 96 pp 10–17*

The authors present an algorithm that provides all factorisations of a polynomial modulo a prime power in probabilistic polynomial time, so long as the prime power does not divide the discriminant.

061709 'Space/Time Trade-Offs for Higher Radix Modular Multiplication Using Repeated Addition'
CD Walter, *IEEE Transactions on Computers v 46 no 2 (Feb 97) pp 139–141*

Using a higher radix in modular multipliers allows a direct trade-off between space and time: chip area is about proportional to speed. In addition, there is an initial (though short-lived) improvement in efficiency when the radix is increased from 2.

061710 'Efficient Exponentiation of a primitive Root in GF(2^m)'
HP Wu, A Hasan *IEEE Transactions on Computers v 46 no 2 (Feb 97) pp 162–172*

The authors develop data structures and algorithms for rapid exponentiation in characteristic two. The exponent is represented as a signed binary or radix-4 number, which enables its weight to be halved; exponentiation can then be done at a reduced gate count with the help of bidirectional shift registers.

8 Theoretical Cryptology

061801 'Average and randomised complexity of distributed problems'
N Allenberg-Navony, A Itai, S Moran, *SIAM Journal of Computing v 25 no 6 pp 1254–1267*

Yao's lemma that the average complexity of the best deterministic algorithm for a problem lower bounds the complexity of randomised algorithms does not apply to distributed systems, as all the processors might run the same instance of the program rather than randomly chosen ones. However, it can be extended under a suitable restriction — componentwise distinct inputs.

061802 'Visual Cryptography for General Access Structures'
G Ateniese, C Blundo, A De Santis, DR Stinson, *Information and Computation v 129 no 2 (15/9/96) pp 86–106*

The authors improve the k-out-of-n threshold scheme for visual cryptography given by Naor and Shamir in **032134** and give a best possible scheme for 2 out of n. They also provide two ways of doing visual cryptography with arbitrary access structures, and prove bounds on the size of the share.

061803 'Locally Random Reductions: Improvements and Applications'
D Beaver, J Feigenbaum, J Kilian, P Rogaway, *Journal of Cryptology v 10 no 1 (Winter 97) pp 17–36*

This is a journal version of a Crypto 90 paper linking locally random reductions with zero knowledge proof.

061804 'Randomness in distribution protocols'
C Blundo, A De Santis, U Vaccaro, *Information and Computation v 131 no 2 (15/12/96) pp 111–139*

The authors analyse the amount of randomness needed by secret sharing and key agreement schemes. They give various upper and lower bounds, and prove the optimality of a scheme presented in **021807**.

061805 'Oblivious Transfers and Intersecting Codes'
G Brassard, C Crépeau, M Sántha, *IEEE Transactions on Information Theory v 42 no 6 (Nov 96) pp 1769–1780*

The authors show that the oblivious transfer of one out of two k-bit strings can be implemented with $\Theta(k)$ calls to a one out of two bit oblivious transfer primitive, and that this is optimal up to a small multiplicative constant. Their construction uses 'zigzag' functions based on self-intersecting codes.

061806 'The wakeup problem'
MJ Fischer, S Moran, S Rudich, *SIAM Journal of Computing v 25 no 6 (Dec 96) pp 1352–1357*

The authors pose the wakeup problem: to design a t-resilient protocol for n asynchronous processes that causes p of them to eventually learn that at least q of them have woken up and started to participate. Applications include security recovery, and equivalent problems are shown to include leader election and consensus. A lower bound is given on the number of shared memory values needed in a shared memory model of computation.

061807 'Threshold computation and cryptographic security'
YJ Han, LA Hemaspaandra, T Thierauf, *SIAM Journal of Computing v 26 no 1 (Feb 97) pp 59–78*

The authors compare the bounded-error probabilistic class BPP with the analogous class for threshold machines, and show that the latter is strictly more powerful if P $\neq$ NP. They define a database to be secure if an adversary watching queries gains

no information except possibly their length, and show that in both the classical and threshold models, if there is any database for which this definition does not coincide with oblivious database access, then P $\neq$ PSPACE.

061808 'A dynamic secret sharing scheme with cheater detection'
SJ Hwang, CC Chang, *ACISP 96 pp 48–55*

In a dynamic threshold scheme, the dealer can renew the value of a secret by public broadcast. This paper describes one such scheme that allows detection of cheating by shareholders. It has 3 parts: in the construction part the dealer collects some public information provided by participants and constructs a public table that assigns values to each participant; in the reconstruction part, when the value of the secret is changed when the public table is modified; in the recovery part a group of t participants recover the secret. The system is shown to overcome the shortcomings of some previous ones.

061809 'A Language-Dependant Cryptographic Primitive'
T Itoh, Y Ohta, H Shizuya, *Journal of Cryptology v 10 no 1 (Winter 97) pp 37–49*

The authors discuss relationships between the opacity or transparency of the functions induced by a language and the kinds of zero-knowledge proof that exist for it.

061810 'Key Sharing Based on the Wire-Tap Channel Type II Concept with Noisy Main Channel'
V Korjik, D Kushnir, *Asiacrypt 96 pp 210–217*

The information obtained by an eavesdropper about a key shared by two legitimate users, with the eavesdropper obtaining s bits of her choice from all n bit blocks ($n > s$) transmitted on a noisy channel, is considered. The eavesdropper's initial knowledge of the key may be partial or none.

061811 'Towards Characterizing When Information-Theoretic Secret Key Agreement Is Possible'
U Maurer, S Wolf, *Asiacrypt 96 pp 196–209*

The authors consider the problem of establishing a secret key between A and B over an insecure channel, where information of an eavesdropper E would be arbitrarily small. For random variables X, Y, and Z, known to A, B, and E, respectively, where all the variables result from a binary random variable sent through three independent channels, the secret key agreement is possible iff $I(X;Y|Z) > 0$.

061812 'An Alternative Model of Quantum Key Agreement via Photon Coupling'
Y Mu, Y Zheng, *ACISP 96 pp 320–331*

The authors describe using a signal generator to produce four non-orthogonal states and measuring these signal states with a beam-splitter. They outline a protocol for establishing a common key from these measurements.

061813 ' "Plug and play" systems for quantum cryptography'
A Muller, T Herzog, B Huttner, W Tittel, H Zbinden, N Gisin, *Applied Physics Letters v 20 no 7 (17/2/97) pp 793–795*

Fluctuations in polarisation force many existing quantum cryptosystems to be recalibrated after a few tens of minutes. This may not be an issue in research systems, but would seriously hamper their commercial deployment. The problem can be solved by time multiplexing; the interfering pulses follow the same physical path but are separated by a short time delay. The use of Faraday mirrors automatically compensates for birefringence effects and polarisation dependent losses.

061814 'Quantum cryptography over 23km in installed under-lake telecom fibre'
A Muller, H Zbinden, N Gisin, *Europhysics Letters v 33 no 5 (1996) pp 335–339*

The authors describe a quantum cryptosystem using polarisation encoding that

they tested on a 22.7 km length of installed telecomms fibre. This showed that the system was feasible, but there was high polarisation instability at times.

061815 'Visual Cryptography II: Improving the Contrast Via the Cover Base'
M Naor, A Shamir, *Protocols 96 pp 197–202*

A new model for visual cryptography is presented. Instead of using two transparencies as in **032134**, two sets are used. Each pixel of the original image is mapped into c sub-pixels, the order of stacking the transparencies is significant, and two schemes — for monochromatic and bi-chromatic construction — are presented. The new model should provide much improved contrast, of about $1 - 1/c$; but it does not appear to support general k out of n threshold schemes.

061816 'A nonlinear secret sharing scheme'
A Renvall, CS Ding, *ACISP 96 pp 56–66*

A secret sharing scheme is called linear if a share is a linear combination of the secrets and a number of other randomly chosen variables. This paper describes a nonlinear threshold scheme in which non-access groups may learn information about the secret but this is a computationally difficult task. The system is based on the theory of quadratic forms and allows cheater detection if enough shareholders collaborate.

061817 'The access structure of some secret-sharing schemes'
A Renvall, CS Ding, *ACISP 96 pp 66–78*

This paper reviews the two main approaches in constructing a secret sharing scheme from a linear error correcting code, and presents a number of results on finding the access structure of a given code. It argues that finding the access structure in a general code is more difficult than finding the weight distribution of the code and hence is a hard problem. Maximum distance separable codes are exceptions; both their weight distributions and access structures are known. For applications that involve small numbers of participants, short linear codes are required and the access structure can be found by brute force.

061818 'A Hidden Cryptographic Assumption in Non-Transferable Identification Schemes'
K Sakurai, *Asiacrypt 96 pp 159–172*

The author discusses a four-pass zero-knowledge protocol of Satoh and Kurosawa for the quadratic residuosity problem. Relations to the Fiat-Shamir protocol are discussed and a new concept of soundness is suggested.

061819 'Non-repudiation without public-key'
R Taylor, *ACISP 96 pp 27–37*

Non-repudiation techniques mainly use digital signatures and are thus computationally secure. In this paper, Taylor's unconditionally secure non-repudiation scheme (**032826**) is further developed. It is optimised to maximise the number of messages that may be sent with a given amount of shared key and to reduce the amount of key information that must be held by the arbiter. However, the cost of this is a loss of unconditional security.

061820 'On a Special Class of Broadcast Channels with Confidential Messages'
M van Dijk, *IEEE Transactions on Information Theory v 43 no 2 (Mar 97) pp 712–714*

The author reinterprets Csisár and Körner's characterisation of noisy memoryless channels in terms of mutual information, and applies it to the wiretap channel. This enables him to prove that if the channels from the sender to the receiver and the eavesdropper are both symmetric, discrete and memoryless, then the secrecy capacity between the sender and receiver is precisely the difference in capacity between the channels to the receiver and the eavesdropper.

061821 'Interferometry with Faraday mirrors for quantum cryptography'
H Zbinden, JD Gautier, N Gisin, B Huttner, A Muller, W Tittel, *Electronics Letters v 33 no 7 (27/3/97) pp 586–587*

The authors describe creating a secret key at a rate of 0.5 bit/sec over almost 23 km of installed telecommunications fibre. The main engineering problem of previous quantum cryptosystems had been maintaining alignment of the polarisers or interferometers; this was solved by making both the interfering pulses travel the same path.

9 Book Reviews

'CHINESE REMAINDER THEOREM'
Cunsheng Ding, Dingyi Pei, Arto Salomaa
World Scientific Publishing Co. (Singapore), ISBN 981-02-2827-9

This book tells the history of the Chinese Remainder Theorem from its first appearance in an arithmetic manual of Sun Zi in the first century and its rediscovery by Fibonacci in the thirteenth. The original Chinese applications had been architectural (deciding whether a given structure could be assembled from bricks, stones and doors of given dimensions without cutting any of them) and military (counting the number of soldiers in an army by getting them to stand in rows of different lengths, and counting the remainders).

More modern applications to computing, cryptology and coding theory form the bulk of the text. In addition to the well known algorithmic applications in cryptosystems such as RSA, there are surprisingly many algorithmic problems in which Chinese Remainder techniques are efficient, especially when extended from the rational integers to polynomial rings: examples in the book are drawn from spectral transforms and convolutional coding.

In addition to the historical background and interdisciplinary insights, the book contains an original treatment of the relationships between secret sharing schemes, error correcting codes and correlation immune Boolean functions. Finally, there is a survey of public key systems based on knapsacks with respect to composite moduli.

This book will be valued by cryptomathematicians for pointing out many novel or little known relationships between these different topics.

How to Subscribe

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

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

Back issues offer: Get a subscription for 1997 (volume 6) plus a set of the remaining back numbers (currently volumes 2 through 5) at a price of £90 for individual subscribers and £145 for corporate subscribers. Electronic copies of back numbers over a year old are at `http://www.cl.cam.ac.uk/users/rja14`.

Individual subscription for 1997 — Please debit my VISA/MasterCard £60 □ I enclose a cheque for £60 □ / US$90 □

Individual subscription for all available 1993–1997 issues — Please debit my VISA/MasterCard £90 □ I enclose a cheque for £90 □ / US$135 □

Corporate subscription for 1997 — Please debit my VISA/MasterCard £95 □ I enclose a purchase order / cheque for £95 □ / US$142.50 □

Corporate subscription for all available 1993–1997 issues — Please debit my VISA/MasterCard £145 □ I enclose a purchase order / cheque for £145 □ / US$212.50 □

Name: .....

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

Cardholder Address: .....

.....

.....

Delivery address (if different) .....

.....

.....

Email address: .....

Signature: .....

We can accept email credit card orders, but some card issuers insist that your card number and expiry date be encrypted. You can use PGP; a key with fingerprint `E5C7 93BE 379D 2842 49DC A809 A147 05F6` can be fetched from `http://www.cl.cam.ac.uk/users/rja14`. You can also fax this order form to us on +44 1223 334678, or mail it to us at:
Northgate Consultants Ltd., 10 Water End, Wrestlingworth, Sandy, Beds SG19 2HA, United Kingdom