Computer and Communications

Security Reviews

Volume 1 Number 1 December 1992

CONTENTS

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

Address for subscriptions: Northgate Consultants Ltd., Ivy Dene, Lode Farm, Lode, Cambridgeshire CB5 9HF, United Kingdom. Annual subscription £60 or $95.

1 Applications and Engineering

MJ Beller, Y Yacobi, *Eurocrypt 92*
'Batch Diffie-Hellman Key Agreement Systems and their Application to Portable Communication'

A variant of Diffie Hellman is proposed to set up keys between secure portable telephones and the exchange. A common composite modulus is used whose factorisation is known only to the exchange; the public keys are short; and the secret keys are all provided by the exchange.

CH Bennett, F Bessette, G Brassard, L Salvail, J Smolin, *J. of Cryptology v 5 pp 3 - 28*
'Experimental Quantum Cryptography'

The principle of quantum cryptography is that two parties can use the Heisenberg uncertainty principle to estimate the amount of eavesdropping which has taken place on a channel and (if this is low enough) derive a number of absolutely secret shared random bits. This paper describes the first implementation of the principle and the results obtained, including the effect of eavesdropping. It is suggested that the technology may eventually be practical, in particular for secure distributed computing.

D Chaum, *Scientific American, August 1992 pp 76 - 81*
'Achieving Electronic Privacy'

This article explains digital signatures and transaction blinding for a general scientific audience. It describes how personal cryptographic devices can be constructed with integral tamper-proof chips, called observers, to prevent cheating while still permitting users to preserve their transaction privacy with psudonyms.

R Clarke, *Australian Computer Journal v 23 no 1 pp 22*
'Case study Cardomat/Migros - an open EFT/POS system'

This paper describes both the technical and business aspects of a project to implement eftpos in Switzerland's Migros chain of supermarkets during 1986-91. It goes into some detail on the customer requirements, the costs and the benefits of the exercise: the main benefit was reducing payment handling costs from some SFr2 - 3 for cheques to SFr0,20 - 0,80 for EFT/POS; and the second was cutting transaction time at the checkout from 2 minutes to 30 seconds. Pre-authorisation is used to achieve this: the customer enters her card and PIN while her goods are being totalled, gets an authorisation, and only needs one keystroke to approve the final amount. The system, which is based on in-store concentrators, accepts both magnetic cards and chipcards; the latter are expected to become the future standard for various security and service reasons.

GI Davida, YG Desmedt, *Computers and Security v 11 pp 253 - 358*
'Passports and Visas versus IDs'

Most proposed electronic ID schemes are not suitable for use in electronic passports because of two basic requirements: that a passport must carry a physical description, and that it must be endorsable with visas. Two ways to enable this are discussed: an append-and-read-only memory (whose access may be restricted to countries), and a link to a separate device issued by the country to be visited.

TP De Vries, *Computers and Security v 11 pp 315 - 325*
'The Implementation of TSS'

The author gives an implementer's views of the IBM TSS (475x) products range, and explains the use of key control vectors to provide separation of duties, non-repudiation, and other benefits. He describes in particular how the products can be used to implement workstation security.

C Dwork, M Naor, *Crypto 92*
'Pricing via Processing or Combatting Junk Mail'

Junk mail could be discouraged by forcing callers to compute a difficult function such as extracting modular square roots. A trapdoor in this function could be used to allow 'authorised' bulk mail such as conference notification.

N Ferguson, J Bos, *Eurocrypt 92 rump session*
'RSA Library for Smartcard'

This reports the development of an RSA library for a Philips smartcard, which implements 512 bit RSA and provides key generation, encryption and signature functions. Block processing times range from 0.47 to 1.55 seconds.

IG Graham, SH Wieten, *Computers and Security v 11 pp 237 - 244*
'The PC as a Secure Network Workstation'

The authors describe the implementation of workstation security at the Nederlandsche Middenstandsbank using Eracom PC encryptor boards. All disk data were encrypted and key management was based on host faciliies, plus chipcards for use when offline; this infrastructure was used to support access control and a DOS shell.

D Gritzalis, S Katsikas, J Keklikoğlu, A Tomaras, *Computers and Security v 11 pp 149 - 161*
'Determining Access Rights for Medical Information Systems'

A survey was carried out to determine the attitudes of the Greek medical community to information security, with a view to formulating an access rights policy which would be widely accepted. Staff attitudes towards who should have access to medical records, diagnoses, bills, and the cost of tests and drugs were determined and are presented. From this, an access matrix for medical information systems is derived.

R Heiman, *Eurocrypt 92*
'Secure Audio Teleconferencing - Practical Solutions'

Bridges in digital secure audio systems have to add signals, which can cause problems if the participants don't want to share secrets with the bridge. One previous approach (Brickell et al, Crypto 89) was to add a random bitstream to encrypt, and subtract a multiple of it to decrypt. The article criticises this as suffering from synchronisation problems, being vulnerable to energy level detection by an opponent, and needing linear encoding (rather than the usual logarithmic scheme). An alternative is proposed in which the bridge relays the maximum of the two bitstreams. This gives acceptable audio quality; but the bridge can still work out who is talking when unless an idle signal is added.

R Hirschfeld, *Crypto 92*
'Making Electronic Refunds Safer'

This paper discusses an electronic cash protocol of Chaum, Fiat and Naor, which allows a coin to be both spent and refunded. Chaum's suggestion was to penalise detected cheaters; this is criticised as being hard to justify in practice. Instead, a modification is proposed to the protocol.

IEEE Communications Magazine (Special Issue) v 30 no 1 (Jan 92)
'Role of Communications in Operation Desert Storm'

A series of overlapping articles in this magazine describe, from a number of points of view, the communications systems used in Operation Desert Storm: a huge tactical communications network was created in a short space of time using satellites, radio links and leased lines. Experts from various US armed services claim that the effect of communications capability on the war was absolutely decisive. The use of encryption devices on LANs and packet switch networks is described, without much detail. Future US military communications strategy entails a wide diversity of terminal equipment on a common network with open architecture but multilevel security.

GJ Kühn, *Proc. 1992 South African COMSIG, p 165 - 168*
'The use of secret-key techniques in forward information verification'

This paper gives an overview of Simmons' theory of authentication and shows how it may be applied to evaluating designs for electricity prepayment meters.

LM Paoletti, *Computer Communications Review v 27 no 1 pp 82 - 94*
'The Department of Defense Communications in the 21st Century'

The Defence Communications Agency operates many networks for the US Department of Defense and is one of the world's largest users of data and voice communications; terminal equipment includes about 100,000 STU-III secure phones and 500,000 PCs at facilities in 75 nations. Cryptography is used at several layers to provide access control to communications, devices and applications. The strategy for fixed (as opposed to tactical and strategic) networks is to minimise the huge administrative load by creating one integrated network out of standard components.

TB Pedersen, D Chaum, *Crypto 92*
'Wallet Databases with Observers'

If an electronic wallet is controlled by the customer, there are potential correctness problems, as the customer might delete a negative credential, or spend money twice. On the other hand, if the wallet is controlled by a bank, it could easily compromise the customer's privacy. The proposed solution is to split the wallet into two units: a customer device C, such as a handheld computer, to safeguard privacy, and a tamperproof unit T, such as a smartcard, issued by the bank. Protocols are presented whereby T and C work together to provide both privacy and correctness. An open problem is whether all messages can be blinded, so that the return of T to the bank will not leak information on the transaction history.

A Pfitzmann, B Pfitzmann *Advances in Medical Informatics pp 368 - 386* **'Technical Aspects of Data Protection in Health Care Informatics'**

This article examines the privacy, accuracy and availability issues raised by medical information systems. Sample medical networks are described, including advice databases, home monitoring systems and multimedia systems, and their requirements are discussed. The authors suggest standardising industry protocols, and doing more research on applying anonymity techniques such as Chaum's credential mechanism to ensuring selective confidentiality.

2 Operating System and Database Security

CC Chang, CH Lin, CT Lee, *Information Sciences v 64 pp 35 - 48'*
'Hierarchy Representations Based on Arithmetic Coding for Dynamic Information Protection Systems'

Hierarchical relationships between users may be enforced in access privileges. A convenient way of representing them is to use arithmetic coding, under which entities are allocated a value c in the unit interval, and the n-th relationship becomes the n-th digit in the decimal (or other) expansion of c.

S. Chokhani, *Comm. ACM v 35 no 7 pp 64 - 75*
'Trusted Products Evaluation'

This article presents an evaluator's view of the US NCSC program for certifying computer security products. It includes a detailed table of the requirements for various product design classes and information on the number of products currently being assessed.

JJ Hwang, BM Shao, PC Wang, *Computer Journal v 35 no 1 pp 16 - 20*
'A New Access Control Method Using Prime Factorisation'

Access matrices of a certain size range can be stored and processed more efficiently by using prime factorisation. Each user is allocated a distinct prime, and each facility has the product of the primes of its authorised users.

JP Kelly, BL Golden, AA Assad, *Networks v 22 no 4 pp 397 - 418*
'Cell suppression: Disclosure Protection for Sensitive Tabular Data'

The authors review the cell suppression techniques used by census bureaux to publish statistical data which yields no information on individuals. They show that in general the cell suppression problem is NP-hard by reducing it to the knapsack problem, and develop techniques to measure the amount of suppression required for given protection ranges. The main results are that sliding protection ranges can significantly reduce this amount compared with traditional schemes, and that network-based flow heuristics can provide near-optimal solutions.

A Laribi, D Kafura, *Computers and Security v 11 pp 57 - 73*
'A Protection Model Incorporating both Authorisation and Constraints'

The authors propose a middle ground between mandatory and discretionary models of control of systems which use inheritance rules to determine the status of derived data. Defining constraints on the use or propagation of authorisations to which they are tagged gives economy of representation, and can be useful in managing revocations or, more generally, environments with multiple authorisers.

GE Liepins, HS Vaccaro, *Computers and Security v 11 pp 347 - 355*
'Intrusion Detection - Its Role and Validation'

The authors discuss the role of intrusion detection routines, and describe 'Wisdom and Sense', a product which operates by summarising usage patterns in a decision tree using an algorithm which strives to mazimise information content in a set of rules. They present test results showing the trade-off between the false alarm rate and the detection rate.

TF Lunt, *Computers and Security v 11 pp 41 - 56*
'Security in Database Systems: A Research Perspective'

This article is a survey of the last five years' research in database security and a list of current research problems. It explains entity and referential integrity, polyinstantiation, the propagation of authorisation and revocation, view authorisations, TCB subsets, and the implications of all these issues for database architectures. The problems are listed as defining operational semantics for multilevel databases, support for classification constraints, preventing undesired inferences, and extending secure database concepts to object-oriented, knowledge-based, and distributed database systems.

MS Olivier, SH von Solms, *Computers and Security v 11 pp 259 - 271*
'Building a Secure Database Using Self-Protecting Objects'

The authors consider the implications of enabling objects in a database to protect themselves. The main problem is that the user-object relationship is clouded by the fact that a user may have many applications and other agents acting on his behalf. The proposal, called 'baggage', is that object profiles should propagate through processes, so that output carries profiles of all the input data used.

EH Spafford, *Computers and Security v 11 pp 273 - 278*
'OPUS: Preventing Weak Password Choices'

It may be advantageous to check all user selected passwords against a large list of forbidden choices, which includes common words, previous choices and so on. A very efficient way of storing such a list is provided by a Bloom filter, which is described. Approximately sevenfold compression can be achieved with a false positive rate of under 1%.

J Wu, EB Fernandez, RG Zhang, *Computers and Security v 11 pp 357 - 369*
'Some extensions to the lattice lodel for computer security'

The authors describe Denning's lattice model of user access rights and the drawback of complex worst-case lattice searching. They discuss possible relaxations of the model, such as removing the requirement for a greatest lower bound, and consider their computational resource implications.

3 Security and Risk Management

JA Adam, *IEEE Spectrum August 1992 pp 21 - 28*
'Threats and countermeasures'

This is an overview of system security threats and countermeasures. Its focus is on viruses, but it also covers the internet Computer Emergency Response Team, Martin Marietta's security awareness program, NSA efforts to develop multilevel secure systems, and the UK Ministry of Defence Chots system.

JB Bowles, CE Petáez, *IEEE Spectrum August 1992 pp 36 - 40*
'Bad Code'

This article reviews the various forms of malicious program code and essays a taxonomy of viruses (whose name is attributed to Adleman), trojans, logic bombs, worms and bacteria.

K Bosworth, *British Telecom Technical Journal v 10 no 2 pp 54 - 60*
'Managing the Personal Computer Virus Problem'

This article gives an overview of PC viruses and describes the policy and organisational problems encountered by British Telecom when implementing anti-virus measures. The strategy adopted was for locally delivered support, but with a central unit for incident analysis and policy formulation.

D Davies, *Computer Fraud and Security Bulletin Jan 92 pp 8 - 14*
'Insuring Computer Risks'

The author reviews the new Lloyds electronic and computer crime policy and finds it outdated in a number of ways. He proposes that insurance be based on the assets controlled by a system, its integrity, and the consequences of non-availability.

R Dixon, C Marston, P Collier, *Computers and Security v 11 pp 307 - 313*
'A Report on the Joint CIMA and IIA Computer Fraud Survey'

This reports a fraud survey carried out for UK management accounting and internal auditing professional bodies. 171 senior financial managers replied to a questionnaire, which was followed up by 30 interviews and 10 case studies. The study found that in almost all cases, a company's financial management assumes responsibility for fraud prevention, often informally; their priorities are checking around the system, in particular validating input and reconciling input with output. Auditing staff, on the other hand, were disposed to emphasise physical security and separation of duties. The main recommendations are more formal responsibility for security; better change control; better education of management and staff; proper use of passwords; and checking random transactions.

JD Hollins, *Computer Fraud and Security Bulletin April 92 pp 13 - 16*
'Policy Implementation at WH Smith's'

This article describes the implementation of an information security policy at a large UK retailer during 1988-1991. The emphasis is turning policy into action by means of training, consciousness raising, procedures, and audits.

B Menkus, *Computers and Security v 11 pp 19 - 23*
'A High Rise Building Fire Case Study'

This article analyses the effects of a fire which gutted eight floors of an office building and its effect on the IT activities of 27 tenants, including the regional HQ of a bank. The fire led to a class action by these tenants against the building's landlord and insurer; contingency planners should not believe landlords' assurances about fire risk. The worst affected tenant was one whose records were still paper-based and were completely destroyed.

RW Perry, *Computer Fraud and Security Bulletin June 92 pp 6 - 9*
'Security in a large networked Unix environment'

This article describes computer security measures at 3i, which include the use of BoKS to enhance unix security with passwords which are half random and half user selected, encryption on leased lines and dialback on modems.

ME Rentill, *Computer Fraud and Security Bulletin Sep 92 pp 7 - 9*
'Security management of distributed unix systems'

Many unix security management problems arise from two sources; that systems are cheap enough to be bought on departmental budgets, and that system administration is often done by inadequately trained and motivated staff. Given the technical complexity of unix networks, central security management is essential.

B Robertson, *Computer Fraud and Security Bulletin July 92 pp 12 - 17*
'The security phase of software development'

This article presents a checklist for security testing of application and systems software. It covers analysis of risks and business control requirements; and specifying tests, including test script generation, error insertion, failure simulation, stress testing, overflow condition checking, and stress loading. Testing staff should have an IT background and a 'hacker' mentality.

RL Sherman, *Computers and Security v 11 pp 128 - 133*
'Biometrics Futures'

The author reviews the state of the art of various biometric technologies, including fingerprints, hand geometry, keystroke and signature dynamics, retinal patterns and voiceprints.

BPM Zajac, *Computers and Security v 11 p 217 - 226*
'Cost effectiveness of antiviral software'

This article gives several model cost-benefit analyses of virus incidents to companies and shows how the purchase of anti-viral software can be subjected to net present value analysis.

4 Legal and Public Policy Issues

JA Adam, *IEEE Spectrum August 1992 pp 29 - 35*
'Cryptography = privacy?'

This article gives an elementary introduction to cryptography and reviews the debate over DES and the proposed digital signature standard. Its high point is a set of answers by the NSA to questions on policy about civilian cryptography, followed by a riposte from Rivest and Bidzos.

C Amery, *Information Security Monitor v 7 no 10 pp 7 - 10*
'The European Commission's Draft Data Protection Directive'

This article discusses the EC's draft directive on data protection, which may lead to a formal directive in 1993 and legislation in 1995. The effect will be to harmonise EC data protection, which in practice means upward to the German level. There are grounds for suppliers to hope that encryption of networks may become the norm, and companies should in any case review risk analysis, authentication and access control meqasures on personal data.

JP Barlow, *Comm ACM v 35 no 7 pp 25 - 31*
'The Electronic Frontier - Decrypting the Puzzle Palace'

This article discusses US public policy towards cryptography including the rôle of the NSA, FBI attempts to facilitate wiretapping, export licensing of cryptographic equipment and the effect of current policy on US business.

M Gehrke, A Pfitzmann, K Rannenberg, *Proc 12th IFIP World Computer Congress 1992 pp 579 - 587*
'Information Technology Security Evaluation Criteria (ITSEC) - a Contribution to Vulnerability?'

ITSEC is described, and a number of criticisms are presented. These include its scope (it covers attacks by users, but not threats from designers, manufacturers, operators and outsiders); its functionality (it does not cover user anonymity and unobservability); and the level of assurance it gives (the strength of algorithms and mechanisms are not addressed adequately, and the correctness of verification tools does not need to be proved). On balance, ITSEC could lead to an increase in exposure if used by inexperienced designers.

W Madsen, *Computers and Security v 11 pp 233 - 236*
'Government-Sponsored Computer Warfare and Sabotage'

This article relates a 1990 request for bids for virus production from the US Army Signal Warfare Center. It considers the practicality and ethics of using viruses in warfare and in business competition, and the use of trojans in exported weapons system which could be used to inactivate them if they were ever turned against the US.

W Madsen, *Computer Fraud and Security Bulletin Feb 92 pp 6 - 10*
'Information Security and Intelligence'

The end of the cold war has shifted the focus of electronic intelligence from military to commercial and industrial targets. The author considers that the internet is a major vulnerability, and that the main threat facing the USA is now Japan. He notes that many Asian countries avoid internet connections via Japan, and suggests that the US information security effort should be redirected, and include better management of US internet domains.

JD Moseley, *EDN August 1992 pp 118 - 122*
'Ruggedised computers'

US defence electronics purchases are some 10% of the total world market in electronics. A significant trend is emerging in this sector: as a result of budget cuts, ruggedised commercial computers are displacing many military computers. This is because of lower cost (typically less than half) and faster delivery dates. The article discusses design factors and environmental requirements.

RL Rivest, ME Hellman, JC Anderson, *Comm ACM v 35 no 7 pp 41 - 52*
'Responses to NIST's Proposal'

The authors present three views of the proposed NIST digital signature standard, in which they criticise the way in which it was adopted, its lack of key exchange facilities, and its key length; and discuss possible alternatives.

R Shaker, *Notices of the AMS v 39 no 5 pp 408 - 412*
'The Agency that Came in from the Cold'

This is an excerpt from a speech by the chief mathematician at the NSA. In it he relates that the agency employs a large number of mathematicians, not just on mathematical tasks but also as programmers and hardware designers, and not just on cryptanalysis but also on speech processing, communications and signal processing. The NSA thus has an interest in a strong US mathematical community and since 1987 has tried to promote this in various ways, including grants for undirected research and summer schools for bright undergraduates.

5 Formal Models and Methods

P Bieber, F Cuppens, *J. of Computer Security v 1 p 99 - 129*
'A logical view of secure dependencies'

The authors analyse the modal operator 'R has permission to know x' and the implications of dependency between the inputs of different subjects. There follow a development of logic and a formal definition of causality (the value of objects B can observe is a function of all his inputs up to that time); the dependencies between non-interference, non-deducibility, causality and generalised non-interference are then explored.

D Longley, S Rigby, *Computers and Security v 11 pp 75 - 89*
'An Automatic Search for Security Flaws in Key Management Schemes'

This article describes a PROLOG program which searches for flaws in key management schemes by means of a search tree whose root is the attack goal. It was used to verify a scheme which had been proposed for use in EFTPOS and which tagged keys with their permitted functionality.

J McLean, *J. of Computer Security v 1 pp 37 - 57*
'Proving noninterference and functional correctness using traces'

Noninterference is the property that no high program at a high clearance level can affect the output of a program at a lower level. Previous workers have proved this property formally from a state machine model using traces of the program modules; the author of this paper shows how to dispense with these models and proceed directly from traces to a proof of noninterference. This is done in two stages, by proving that a specification is noninterfering and then showing that a given program satisfies it.

C Meadows, *J. of Computer Security v 1 pp 5 - 35*
'Applying formal methods to the analysis of a key management protocol'

This paper reports the construction of a formal verification model, based on term rewriting, and its success in detecting a flaw in a secret-key selective broadcast protocol proposed by Simmons. The approach is compared with the use of specification languages, expert systems and modal logics. An amended protocol is shown to be sound.

PV Rangan, *Computers and Security v 11 pp 163 - 172*
'An Axiomatic Theory of Trust in Secure Communication Protocols'

While security is a property of a channel, trust is a property of a relationship between agents; and in the absence of any totally trusted agent, one may try to base trust on a logic of belief. Such a logic is developed for reasoning about trust in communication protocols, which may be iterative or recursive in nature.

RS Sandhu, *J. of Computer Security v 1 pp 59 - 98*
'Expressive power of the schematic protection model'

This paper describes a ticket-based access control formalism, the schematic protection model, and shows that it subsumes the Bell-LaPadula and take-grant models, and grammatical protection schemes. The Bell-LaPadula distinction between mandatory and discretionary controls becomes a condition on the propagation of access rights, which is more suited to analysing the consequences of users' behaviour and specifying policies. Safety (of access right propagation) is decidable provided a can-create relationship is acyclic.

6 Secret Key Algorithms

CM Adams, *Info. Proc. Letters 41 no.2, p 77 - 80*
'On immunity against Biham and Shamir's differential cryptanalysis'

As Biham and Shamir's differential cryptanalysis uses the fact that some S-box input XORs may lead to certain output XORs with high probability, the author proposes designing S-boxes all of whose output XORs are equiprobable. An m by n S-box will have this property if, when represented as a 2^m by n matrix, it has m columns all nonzero linear combinations of which are bent functions.

T Baritaud, H Gilbert, M Girault, *Eurocrypt 92*
'FFT Hashing is not Collision-free'

A collision is exhibited for a hash function based on fast Fourier transforms which was proposed by Schnorr at Crypto 91. The attack is based on the function's limited diffusion properties, takes about 2^{23} computations, and generates multiple collisions.

TA Berson, *Eurocrypt 92*
'Differential Cryptanalysis Mod 2^{32} with Application to MD5'

Differential cryptanalysis is extended from considering changes mod 2 (XORs) to changes mod 2^m. Particular attention is paid to the case m=32 because of its use in hash functions. This allows one to find high probability differentials for shift operations. Finally, some high-probability differentials are exhibited for the various rounds of MD5.

E Biham, A Shamir, *Crypto 92*
'Differential Cryptanalysis of the full 16-round DES'

This paper reports a further refinement of differential cryptanalysis, which for the first time can break DES faster than exhaustive search. The data collection phase requires 2^{47} ciphertexts, of which all but 2^{36} are discarded; computing the key then takes 2^{37} operations. The attack can be parallelised and can be carried out incrementally: each unit of analytic work gives rise to a fixed probability of success, and so even if keys are changed frequently, the likelihood of finding one key for a given amount of work remains essentially constant. The attack is less effective if there is plaintext redundancy: for example, 2^{49} out of the 2^{56} possible ASCII texts would be required for it to succeed.

N Burgess, KV Lever, *IEE Proc. Computers and Digital Techniques, v 139 no 2 pp 131 - 3*
'Fast linear congruential pseudorandom number generators using the Messerschmidt pipelining principle'

The authors point out that linear congruential generators can be parallelised easily to k processors,, as the kth iterate of $x_{n+1} = Ax_n \pmod B$ is given by $X_{n+k+1} = A^{k+1}x_n \pmod B$; and the Wichman-Hill generator can be treated in the same way.

KW Campbell, MJ Wiener, *Crypto 92*
'Strong Evidence that DES is not a Group'

Birthday attacks were performed to find key quadruples such that for fifty randomly chosen ciphertexts C and a fixed message M, $C = E_{K1}(E_{K2}(E_{K3}(E_{K4}(M))))$. It appears highly likely from the work required that DES is not closed under functional composition. Combining these results with Coppersmith's shows that DES is not closed, as the lowest common multiple of the cycle lengths is a lower bound on the order of subgroup generated by DES, and, as this is larger than the total number of DES transformations, it follows that DES cannot be closed.

C Carlet, *Crypto 92*
'Partially Bent Functions'

Bent functions, which are at maximum Hamming distance from linear functions, have a number of applications in cryptography, but are unbalanced and seem to be rare. This paper defines a broader class, the partially bent functions, which are also highly nonlinear but are more numerous and include balanced functions. They include quadratic functions, and indeed generalise many of the quadratic functions' desirable features; and they turn out to be precisely those functions whose domain is the direct sum of two subspaces, the restrictions of the function to which are bent and linear respectively.

M Clausen, *Info. Proc. Letters 41 no.6, pp 291 - 2*
'Almost all boolean functions have no linear symmetries'

It is shown that almost all n-ary boolean functions have a trivial stabiliser under the action of $GL(n, 2)$. This generalises a theorem of Clote and Kranakis to the effect that almost no boolean functions have permutational symmetries.

J Denés, AD Keedwell, *Discrete Mathematics v 106 pp 157 - 162*
'A new authentication scheme based on Latin squares'

Given a Latin square of order q, seen as a quasigroup (Q,*), we can hash a message $a_1, \ldots, a_n$ to b (where the a_i and b are q-ary numbers) by $b = [(a_1 * a_2) * a_3] * \ldots * a_n$. It is shown that all such hash values are equiprobable.

A Di Parto, F Guida, E Montolive, *Electronics Letters v 28 no 2 pp 118 - 120*
'Fast algorithm for finding primitive polynomials over GF(q)'

The minimum polynomials of primitive elements in $GF(q^m)$ are precisely the primitive polynomials of degree m, so given any one such polynomial corresponding to a primitive element α, we can find all the others as the polynomials of α^k (for $\mathrm{GCD}(k, q^m - 1) = 1$). The authors show that the coefficients of these polynomials can be found in time $O(m^2)$ by using the Massey-Berlekamp algorithm.

H Eberle, *Crypto 92*
'A High-speed DES Implementation for Network Applications'

This paper describes a DES implementation in a GaAs gate array which has a throughput of 1Gbit/sec. It is designed for use in low-latency network controllers. In addition, at a cost per chip of $300, brute force solution of single-key DES would take on average 8 days with $1m worth of DES chips (as opposed to 47 days or more with CMOS DES chips).

J Eichenauer-Herrmann, *J. Computational and Applied Mathematics v 40 no 3 pp 345 - 350*
'Construction of inversive congruential pseudorandom number generators with maximum period length'

The Eichenauer-Lehn inversive congruential generator has the relation $x_{n+1} = 1/(ax_n + b) \pmod{m}$ where m is a prime power. It is shown how a and b can be chosen to ensure maximum sequence length.

J Eichenauer-Herrmann, H Niederreiter, *Math. Comp. v 58 no 198 pp 775 - 779*
'Lower bounds for the discrepancy of inversive congruential pseudorandom numbers with power of two modulus'

The Eichenauer-Lehn-Topuzoğlu inversive congruential generator has the relation $x_{n+1} = 1/(ax_n + b) \pmod m$ where $m = 2^n$ and a, b are chosen so that the sequence length is $m/2$. The authors extend previous results for the case $m = p$ to this case. Its performance under the serial test is determined by its discrepancy; and a positive proportion of these generators have discrepancy $O(m^{-1/2})$.

D Erdmann, S Murphy, *Electronics Letters v 28 no 9 pp 893 - 895*
'Hénon stream cipher'

Hénon proposed using a chaotic map to generate a binary keystream sequence. The authors show that the subsequence '1100' never occurs, and that the distribution of the other 4-bit subsequences is far from uniform.

LR Knudsen, *Crypto 92*
'Iterative Characteristics of DES and s^2-DES'

Firstly, the modified S-boxes proposed by Kim at Asiacrypt 91 to increase the resistance of DES to cryptanalysis do not work. Secondly, the differentials used by Biham and Shamir appear to be the best general choice, although their probability varies somewhat with the choice of key.

A Gleeson, *Math. Systems Theory v 25 p 253 - 267*
'Semigroups of Shift Register Counting Matrices'

This paper considers onto maps from the space of infinite binary sequences to itself which is induced by a nonlinear shift register. A semigroup of counting matrices is defined and used to prove various structure results.

JD Golič, *Eurocrypt 92*
'Correlation via linear sequential circuit approximation of combiners with memory'

An attack is shown on a wide class of sequence combiners. The idea is to find linear filters of the output and input of a nonlinear combiner with memory which have the effect of destroying its correlation immunity. An efficient procedure is shown for finding such filters. It is proved that if a boolean function has m bits of memory, then there exist two correlated linear functions of (at most $m + 1$ bits of) its output and input respectively. The effect is to extend correlation attacks to many shift register systems, including systems using summation combiners with more than one carry bit.

JD Golič, *Eurocrypt 92 rump session*
'Generalised Correlation Attack'

An attack is reported on clock-controlled shift register sequences, which are seen as a series of blocks, subjected to various edit operations under a number of constraints. The attack uses a result of Hall and Dowling to construct a metric on edit transformations.

SW Golomb, RE Peile, H Taylor, *IEEE Trans. Info. Theory v 38 no 3 pp 1181 - 1183*
'Nonlinear Shift Registers That Produce All Vectors of Weight t'

All binary vectors of weight up to a given maximum can be generated by a suitably chosen nonlinear feedback shift register. A construction is given, together with examples of weight up to seven.

DH Green, SK Amarasinghe, *IEE Proc. Computers and Digital Techniques v 139 no 4 pp 363 - 371*
'Sequences and arrays derived from nonprimitive irreducible polynomials'

Where the exponent e of an irreducible polynomial of degree m over GF(q) is a proper divisor of $q^m - 1$, this exponent determines the correlation properties of the corresponding sequence. Tables are given of possible exponents for irreducible polynomials of degree ≤ 20 over GF(2) and of degree ≤ 9 over GF(3).

MA Hasan, UK Bhargava, *IEE Proceedings on Computers and Digital Techniques v 139 no 3 pp 230 - 236*
'Division and bit-serial multiplication over $GF(q^m)$'

Multiplication in $GF(q^m)$ can be carried out using the discrete-time Wiener-Hopf equation of degree m over $GF(q)$. A serial multiplication circuit based on this is presented, which uses fewer gates and registers than previous designs. A division algorithm is also given.

K Huber, *IEEE Trans. Info. Theory v 38 no 3 pp 1154 - 1162*
'Solving Equations in Finite Fields and Some Results Concerning the Structure of GF(p^m)'

Coset-cycle methods are developed for finding polynomial roots in fields of characteristic two. The basic idea is that given Zech's logarithm $Z(s)$ of any element s, we can quickly compute $Z(t)$ for all t in the same coset as s; so decompose the target polynomial by cosets. The algorithm appears to have time complexity O(d^2m) for polynomials of degree d in GF(2^m). It can also be applied in fields of larger characteristic, but is less efficient.

X Lai, JL Massey, *Eurocrypt 92*
'Hash Functions Based on Block Ciphers'

This paper classifies attacks on hash functions according to whether they have a target hash value or merely seek a collision, and according to how much freedom the analyst has to choose the input message. It then considers hash functions constructed by iterating block ciphers in various ways and analyses their security against these kinds of attack.

HT Liaw, CS Lin, *IEEE Transactions on Computers v 41 no 6 pp 661 - 664*
'On the OBDD-Representation off General Boolean Functions'

This paper describes the use of ordered binary decision diagrams (OBDDs) to represent boolean functions. OBDDs can be reduced in many cases by merging isomorphic subgraphs; some important functions such as multiplication have OBDDs which grow exponentially in the input size, but the worst case growth is $(2^n/n)(2+\epsilon)$. Almost no OBDDs are sensitive to variable ordering.

S Lloyd, *J. of Cryptology v 5 pp 107 - 131*
'Counting Binary Functions with Certan Cryptographic Properties'

This article reviews and develops the characterisation of boolean functions of n variables which are balanced, satisfy the $(n-3)$ strict avalanche criterion (SAC), and have a given degree of correlation immunity. It is shown that $(n-3)$ SAC functions are determined by (and can be calculated as products of) their values on inputs of weight less than 3. It turns out that for $n \geq 9$, most functions have these three properties.

PK Lui, JC Muzio, *Int. J. Electronics v 72 no 1 pp 21 - 35*
'Structure of modulo-2 ring-sum canonical expressions for boolean functions'

New algebraic and geometrical representations of boolean functions are developed which relate expansion coefficients to subfunctions in the parity spectrum. This spectrum can be displayed as a hypercube, which gives us algorithms to find an implementation using a minimal number of gates.

M Matsui, A Yamagishi, *Eurocrypt 92*
'A New Method for Known Plaintext Attack of FEAL Cipher'

An attack is presented which breaks FEAL-4 with 5 known plaintexts and FEAL-6 with 100. The method can be extended to break FEAL-8 faster than exhaustive search given 2^{15} plaintexts. The technique works by constructing a check function which enables us to search for part of the key at a time.

UM Maurer, *J. of Cryptology v 5 pp 53 - 66*
'Conditionally-Perfect Secrecy and a Provably-Secure Random Cipher'

If there exists a publicly available source of random bits whose length exceeds that of all messages to be encrypted, then an almost perfectly secure cryptosystem can be constructed whose keylength is much less than the message length. This uses a keystream formed as the sum of subsequences of the random bits, addressed by a short secret key. In the case where the random bits are broadcast, the cipher might be provably secure on the assumption that the opponent has finite memory (without the secret key, he does not know which subsequences to store).

UM Maurer, *J. of Cryptology v 5 pp 89 - 105*
'A Universal Statistical Test for Random Bit Generators'

A new test is proposed for random bit generators which measures to what extent their output can be compressed. The test parameter is the average of the log of the distances between occurrences of the same block; the sequence will pass if it can't be significantly compressed by source coding. This test has the properties that it measures the per-bit entropy, and will reject sequences which fail the serial and runs tests; however it is not sensitive to a small bias in the frequency of 0 and 1, and so cannot replace the frequency test.

UM Maurer, *Eurocrypt 92*
'A Simplified and Generalised Treatment of Luby-Rackoff Pseudorandom Permutation Generators'

This paper reviews the work on pseudorandom permutations which has followed the Luby-Rackoff paper on this topic. If we have a black box which contains a random function and a set of pseudorandom functions, can we distinguish between them? Two types of limit are possible on the distinguisher: if she is limited to polytime, complexity theory applies: if the number of arguments she can sample is restricted, probability theory applies. It goes on to show that suitable pseudorandom permutations can be constructed from locally random functions.

W Meier, O Staffelbach, *J. of Cryptology v 5 pp 67 - 86*
'Correlation Properties of Combiners with Memory in Stream Ciphers'

This paper extends correlation attacks to combiners with memory. It is shown that memory does not greatly reduce the total correlation, which remains largely independent of the combiner, but merely allows one to redistribute it. A general analysis is given of combiners with one bit of memory. In addition, the uncertainty about this carry bit is reduced if we know an amount of the output sequence. These results are combined to give a fast attack on the two input summation combiner.

AJ Menezes, PC van Oorschot, SA Vanstone, *SIAM J. Computing v 21 no 2 pp 228 - 239*
'Subgroup refinement algorithms for root finding in $GF(q)^*$'

This article surveys root-finding algorithms in $GF(q)^*$ and proposes an improved version of the Moenck method, which, for smooth $q-1$, and given any primitive root, will find a root for a polynomial in polytime by searching successively refined sets of coset cycles.

MJ Mihajlevič, JD Golič, *Eurocrypt 92*
'Convergence of a Bayesian iterative error-correction procedure to a noisy shift register sequence'

A Bayesian iterative error-correcting procedure is proposed for correlation attacks on shift register sequences. It can be used to reconstruct the initial state of the shift register if and only if the noise probability is less than a function of the number of parity checks. Two similar estimates are given for this function: the first is derived from the self-composition of the Bayes error probability, and the second from the convergence of the sequence of residual error rates.

CJ Mitchell, *IEEE Transactions on Computers v 41 no 4 pp 505 - 507*
'Authenticating Multicast Internet Electronic Mail Messages using a Bidirectional MAC is Insecure'

The bidirectional MAC proposed in Internet RFC989 consists of two 64-bit DES MACs, one computed backward and the other forward. This is not adequate: a birthday attack is shown which requires about 2^{33} MAC operations, and for which certain time-space tradeoffs are possible.

H Niederreiter, *Czechoslovak Math. Journal v 42 no 117 pp 143 - 166*
'Low-discrepancy point sets obtained by digital constructions over finite fields'

Point sets in the unit cube are defined by coordinates expressed as sequences of digits to a prime power base; the digits are generated systematically by a set of shuffling functions, which can be evaluated using shift register sequences. These sets are shown to have low discrepancy.

H Niederreiter, CP Schnorr, *Eurocrypt 92*
'Local Randomness in Candidate one-way functions'

The authors define a measure of local randomness on strings and characterise families of polynomials over Z_n whose least significant bits are locally random. These are suggested as candidates for the construction of hash functions.

K Nyberg, *Eurocrypt 92*
'On the construction of highly nonlinear permutations'

The nonlinearity of a permutation of a vector space over a finite field can be measured as its Hamming distance from any affine function; this is independent of the choice of basis. It is shown that quadratic forms are very nonlinear in this sense, and that a permutation is similarly nonlinear iff every nontrivial linear combination of its coordinate functions is a balanced quadratic form. An efficient construction for nonlinear permutations can be derived, using a result of Pieprzyk that the trace of a cubic function on $GF(2^n)$ is quadratic for N odd.

L O'Connor, *Eurocrypt 92*
'Suffix Trees and Sequence Complexity'

The span of a sequence is the length of the shortest (not necessarily linear) feedback shift register which generates it, and the size of a feedback shift register is the number of terms needed to describe it. The paper shows that if a sequence is encoded in a suffix tree, then its span is the longest path from the root to a certain type of leaf. From this, it follows that the span is usually less than the linear complexity, but the size of the corresponding nonlinear generator seems to grow exponentially, and so is usually larger than the size of the smallest linear feedback shift register which generates the sequence. Supporting numerical results are presented for 100,000 randomly chosen 32-bit sequences.

J Patarin, *Eurocrypt 92*
'How to construct pseudorandom and superpseudorandom permutations from one single pseudorandom function'

If f is a pseudorandom function, then $\psi(f, f, f \circ \zeta \circ f)$ is pseudorandom, and $\psi(f, f, f, f \circ \zeta \circ f)$ is superpseudorandom, for a suitable well chosen permutation ζ. The key idea in the proof is the notion of the 'spreading' of the permutation, which is the maximum number of solutions of $x \oplus \zeta(x) = K$ over all K.

D Roelants van Baronaigen, F Rusky, *Discrete App. Math. v 36 pp 57 - 65*
'Generating permutations with given ups and downs'

An efficient algorithm is presented to generate all permutations of a given signature, which is equivalent to generating all topological sortings of a poset whose Hasse diagram is a path. Permutations are represented using sequences which order them lexicographically.

CP Schnorr, *Eurocrypt 92*
'FFT-hash II, Efficient Cryptographic Hashing'

This presents an improved version of the hash function presented at Crypto 91 and subsequently broken. Its design motivations are that polynomial mappings on finite fields provide good local randomness, and that fast Fourier transforms are much less timeconsuming then multiplying large integers.

B Sadeghian, J Pieprzyk, *Eurocrypt 92*
'A construction for Super Pseudorandom Permutations from a Single Pseudorandom Function'

It is shown that $\psi(g, 1, f, g, 1, f)$ is superpseudorandom, as is $\psi(f^2, 1, f, f^2, 1, f)$ provided the number of oracle gates in the distinguishing circuit is limited. A resulting open problem is the status of $\psi(f, f^2, f, f, f)$ and whether such structures can be used to strengthen practical block ciphers.

SE Tavares, M Sivabalan, LE Peppard, *Crypto 92*
'On the Design of SP Networks from an Information Theoretic Point of View'

The authors develop the concept of information leakage to study the quality of S-boxes in substitution-permutation networks. The criterion is that information about input bits should not reduce the uncertainty of an unknown output bit or vice versa. An equivalence relation can be defined on S-boxes enabling us to get a large number of these for every 'desirable' one we construct. Numerical results suggest that a good choice of S-boxes has the effect of minimising the number of rounds required to achieve optimal security.

R Wernsdorf, *Eurocrypt 92*
'The One-round Functions of DES Generate the Alternating Group'

Each round of DES consists of 2^{48} permutations. The group which they generate is shown to be 3-transitive, and if this were not equal to $A_{2^{64}}$, then it would have a unique minimal normal subgroup which is Abelian or simple. The former is excluded by displaying a permutation with too many fixed points, and the latter by the classification theory of simple groups.

7 Public Key Algorithms

M Alabaddi, SB Wicker, *Electronics Letters v 28 no 9 pp 890 - 891*
'Security of Xinmei's digital signature scheme'

The Xinmei digitial signature scheme, which is based on (n,k) Goppa codes, can be attacked given $n+1$ linearly independent signed copies of the same message. It then reduces to the solution of linear systems of equations taking time $O(n^3)$.

M Alabaddi, SB Wicker, *Electronics Letters v 28 no 18 pp 1756 - 8*
'Cryptanalysis of the Harn and Wang modification of the Xinmei digital signature scheme'

The Harn-Wang variant of the Xinmei signature scheme based on (n,k) Goppa codes is vulnerable to a known plaintext attack which takes time $O(k^3)$.

RJ Anderson, *Electronics Letters 28 no 15 (7/92) p 1473*
'Attack on server assisted authentication protocols'

Server-aided protocols enable a device such as a smartcard to speed up computations using insecure auxiliary devices. A protocol of Matsumoto, Kato and Imai is shown to be insecure: instead of returning partial signatures for the desired message, the server can instead send back a set of values designed to discover the card's secret key. The implication is that the smartcard must check the signature before releasing it, and this makes such protocols less practical.

T Baritaud, M Campara, P Chauvaud, H Gilbert, *Crypto 92*
'On the Security of the Permuted Kernel Identification Scheme'

A time-memory tradeoff is shown for attacks on Shamir's permuted kernel scheme. This consists of precomputing and sorting the contributions made by a number of the rows of the public matrix and the permutations of a subset of the target public key vector, and then performing exhaustive search on the remaining public key components. During this search, we can discard any permutation whose contribution from any matrix row is not a value in our list. The effect is that a system with a modulus of 251 and a 16 by 32 public matrix can be broken in time 2^{56} and memory 2^{47}, rather than the 2^{76} time complexity previously claimed.

J Bos and D Chaum, *Crypto 92*
'Provably Unforgeable Signatures'

This paper combines the concepts of a combinatorial signature scheme and a one-time pad to produce practical signatures which are provably secure (on the assumption that RSA is). Each signer publishes a modulus n which he can factor, and precomputes secret values $m_{ij} = r_j^{1/p_i} \pmod{n}$ for a public list of prime numbers p_i and random numbers r_j. These are used once only to form a signature of the form $S = \prod m_{ij}$ (eg one could use a new prime p_i for each message and encode its bits in the choice of r_j). Provided each combination of primes and random numbers is used only once, the uniqueness of factorisation implies that these signatures are secure against even an adaptive chosen-message attack.

EF Brickell, KS McCurley, *J. of Cryptology v 5 pp 29 - 39*
'An Interactive Identification Scheme Based on Discrete Logarithms and Factoring'

An identification scheme is proposed as follows. Let the authority choose primes p, q so that $q-1$ is divisible by qw but not q^2, where both q and w are large enough not to be guessed, and an element α of order q in Z_p^*; and publish p, α and its public key. Users are registered as follows: each chooses a random s in Z_p^* and presents $v = \alpha^{-s} \pmod{p}$ to the authority, which issues a certificate binding v to their identity. In use, the prover chooses a random r and sends the verifier $\alpha^r \pmod{p}$; the verifier returns a random e; the prover replies with $y = r + se \pmod{(p-1)}$; and the verifier accepts him if $x = \alpha^y v^e \pmod{p}$. The authors show that an algorithm to solve $x = \alpha^y v^e \pmod{p}$ for y can be used to compute the discrete log of v, and that the scheme is witness hiding unless $p-1$ can be factored.

CC Chang, CS Laih, *IEE Proc. Computers and Digital Techniques v 139 no 4 p 372*
'Remote password authentication with smart cards'

The authors show that the Chang-Wu password scheme is unsound; some of the secret centre information can be calculated from the public keys, enabling passwords to be intercepted and compromised.

D Chaum, TB Pederson, *Eurocrypt 92*
'Transferred Cash Grows in Size'

Electronic cash systems which have the property that participants' identities are secure unless they cheat by spending a coin twice, must encode information on each coin about everyone who has ever spent it. Thus the transferred cash grows in size, regardless of whether the security is unconditional or merely computational. Size bounds are discussed, and it is argued that an unbounded opponent could probably always trace coins anyway.

T Chikazawa, A Yamagishi, *Electronics Letters v 28 no 11 pp 1015 - 1017*
'Improved identity-based key sharing system for multiaddress communication'

This paper presents a strengthened version of an identity-based key distribution scheme which was analysed by Shimbo and Kawamura at Asiacrypt 91. It is based on factorisation and discrete log, and has the property that a sender can encrypt a message key for two recipients simultaneously.

JH Evertse, E van Heijst, *J. of Cryptology v 5 pp 41 - 52*
'Which New RSA-Signatures Can Be Computed from Certain Given RSA Signatures?'

An opponent who cannot extract RSA-roots mod N can only calculate new signatures which are products and quotients of existing signatures. This is extended to the situation where one message is signed with a number of secret keys corresponding to known public keys; the opponent can only compute signatures which can be checked by public keys which are in the Abelian group generated by the known keys.

JH Evertse, E van Heijst, *Eurocrypt 92*
'Which new RSA signatures can be computed from RSA signatures, obtained in a specific interactive protocol?'

In digital cash protocols, the user may choose a blinding factor before getting an instrument signed by the bank. This raises the question of whether he can defraud the system by influencing the signatures he receives. For a specific protocol, this turns out to depend on whether a particular quadratic matrix equation is soluble in integers.

J Georgiades, *J. of Cryptology v 5 pp 133 - 177*
'Some Remarks on the Security of the Identification Scheme Based on Permuted Kernels'

This article starts with a lucid exposition of the permuted kernel scheme and then shows that the security of a 16 by 32 matrix scheme can be reduced from the claimed 2^{76} to 2^{65} by considering equations in the elements of a basis for the kernel. It also shows a cheating strategy with a success probability of 2^{-r} for an r-round protocol.

L Harn, DC Wang, *Electronics Letters v 28 no 2 pp 157 - 159*
'Cryptanalysis and modification of digital signature scheme based on error-correcting codes'

The Xinmei digital signature scheme is vulnerable to forgery because of its linearity; valid signatures of messages can be combined using exclusive or to give a valid signature for the combined message. The authors propose repairing this weakness by hashing messages before signature.

G Harper, A Menezes, S Vanstone, *Eurocrypt 92*
'Public Key Cryptosystems with Very Small Key Lengths'

An elliptic curve cryptosystem is presented which is based on $y^2 + xy = x^3 + ax^2 + b$ over the field $GF(2^{104})$. For a certain choice of a and b, the order of the curve contains a 29-digit prime divisor, and is thus secure against the best known attack (the Pollard ρ method). As keys are only 104 bits long, the system could be used in applications where, for example, the secret key might have to be memorised.

T Hwang, *Info. Processing Letters v 42 no 8 p 83 - 86*
'Attacks on Okamoto and Tanaka's one-way ID based key distribution system'

The Okamoto-Tanaka scheme used secure chipcards to calculate a shared master key for A and B as $MK \oplus ID_A \oplus ID_B$, where MK is a universal master key. This scheme fails, as A can input to his system a composite correspondent identity such as $ID_A \oplus ID_B \oplus ID_C$, and then masquerade as B to C or vice versa. The scheme can be repaired by hashing identities before combining them into keys.

JH Loxton, DSP Khoo, GJ Bird, J Seberry, *J. of Cryptology v 5 pp 139 - 150*
'A Cubic RSA Code Equivalent to Factorisation'

A modified RSA scheme is developed in the ring $Z[\omega]$ of Eisenstein integers where $\omega = \frac{1}{2}(-1 + \sqrt{-3})$ is a primitive cube root of unity. Extracting RSA roots in this scheme is shown to be equivalent to factorising the modulus.

CA Meijer, AR Meijer, *Proc. 1992 South African COMSIG, p 175 - 178*
'A proposed public key bitstream cipher'

This paper proposes to generate a keystream as the binary expansion of a/p where a is established as follows. If user A has private key x_A and public key g^{x_A}, the parties choose random r_A, r_B, exchange g^{r_A} and g^{r_B}, and set $a = g^{x_A r_A + x_B r_B}$.

S Micali, *Crypto 92*
'Fair Public-Key Cryptosystems'

This paper defines a system as fair if it presenves the balance of privacy between a government and its citizens, in the sense that their privacy can be compromised by the government if and only if a court order is obtained. The proposed mechanism is that a number of trustees would each receive a piece of each user's secret key, and would pass these to the authorities on receipt of the appropriate warrant. Variants of Diffie-Hellman and RSA are proposed which have the property that the trustees can verify that they have in fact received all the components of the user's secret key before releasing his public key to a public directory.

T Okamoto, *Crypto 92*
'Provably Secure Practical Identification Schemes and Corresponding Signature Schemes'

The Brickell-McCurley scheme is refined and generalised by using two generators instead of one. This lets us construct three-move identification schemes which are based on, and provably as difficult as, any problem which is random self-reducible in the sense of Tompa and Woll. The method is illustrated for both discrete log and factorisation. In the former case, let p and q be primes with $q \mid (p-1)$; let g_1 and g_2 be of order q in Z_p^*; let each user choose secret s_1, s_2 in Z_q and publish $v = g_1^{-s_1} g_2^{-s_2} \pmod p$. During each protocol run, the prover chooses random r_1 and r_2, and sends the verifier $g_1^{r_1} g_2^{r_2} \pmod p$; the verifier sends a challenge e; the prover responds with $y_1 = r_1 + es_1 \pmod q$ and $y_2 = r_2 + es_2 \pmod q$; and the verifier checks that $x = g_1^{y_1} g_2^{y_2} v^t \pmod p$.

T Okamoto, A Fujioka, E Fujisaki, *Crypto 92*
'An Efficient Digital Signature Scheme Based on an Elliptic Curve Over the Ring Z_n'

A scheme is proposed based on an elliptic curve mod n, $n = p^2 q$. It is an upgrade of a previous scheme by Okamoto which was based on polynomial approximation and which had been broken in the quadratic case. The new elliptic curve variant is secure against the previous attacks, and is much faster than RSA. There are descriptions of two further variants which use rational functions instead of a polynomial.

B Pfitzmann, M Waidner, *Eurocrypt 92*
'Attacks on Protocols for Server-Aided RSA Computation'

Server-aided protocols enable a device such as a smartcard to speed up computations using insecure auxiliary devices. A passive attack is shown on the server-aided protocol of Matsumoto, Kato and Imai. The objective is to determine which elements of a vector have been multiplied together to give a signature; this is achieved by computing all products of up to half the elements, sorting and looking for a match whose components are disjoint. An active attack using Jacobi symbols is also described.

E van Heijst, T Pedersen, B Pfitzmann. *Crypto 92*
'New Constructions of Fail-stop Signatures and Lower Bounds'

Fail-stop signatures have the property that the alleged signer of a forged signature can prove that it is a forgery, even against a computationally unbounded opponent. The basic idea is that the signer chooses at random one of many secret keys corresponding to her public key; as different secret keys give different signatures, a forger who can guess another one will be exposed (the alleged prover can produce another signature to the message, and two different signatures on the same message are treated as proof of forgery). Previous fail-stop schemes had been based on discrete log; this paper proposes a scheme based on factoring.

E van Heijst, T Pedersen, *Eurocrypt 92*
'How to Make Efficient Fail-stop Signatures'

Fail-stop signatures have the property that the alleged signer of a forged signature can prove that it is a forgery, even against a computationally unbounded opponent. This paper proposes a new construction for these signatures which is based on discrete log and is more efficient than previous schemes. The paper also shows how certain undeniable signatures can be converted to fail-stop signatures.

Y Zheng, J Seberry, *Crypto 92*
'Practical Approaches to Attaining Security Against Adaptively Chosen Ciphertext Attacks'

Chosen-ciphertext attacks against public-key cryptosystems are reviewed. It is shown that a previous proposal is vulnerable to an adaptively chosen ciphertext attack. The paper goes on to propose using a hash function to add redundancy to the plaintext, and to program the decryption device to output no plaintext unless this is present.

8 Computational Number Theory

A Balog, C Pomerance, *Proc. AMS v 115 no 1 pp 253 - 267*
'The distribution of smooth numbers in arithmetic progressions'

The number of integers up to n in the progression $a \pmod q$ which have no prime factor greater than B is shown to be $\frac{n}{q}\exp\left(-u(\log u + \log\log u + O(1))\right)$ for a large number of values of a, q and B.

J Brandt, I Damgård, *Crypto 92*
'On Generation of probable Primes by Incremental Search'

If a conjecture of Hardy and Littlewood is true, then the probability that Rabin's test will not find a probable prime among s consecutive k-bit odd numbers is less than $2\exp(-2s/k) - 2\exp(-2s/k - \epsilon)$, and that the uncertainty of primes so found is almost linear in k. This tends to confirm that, in cryptographic applications, using the Rabin test to find primes results in no significant loss of security compared with a uniformly random choice of primes.

E Brickell, DM Gordon, KS McCurley, D Wilson, *Eurocrypt 92*
'Fast exponentiation with precomputation'

Precomputation can be used to speed up the computation of different powers of a fixed element. For $n \leq N$, g^n can be calculated in $O(\log N/\log\log N)$ group multiplications. The possible trade-offs between storage and time are tabulated for $N = 2^{160}$ and 2^{512}. The technique can be adapted efficiently for parallel computation.

JH Davenport, *Proc. ISSAC 92*
'Primality Testing Revisited'

Numbers have been constructed which pass the Rabin primality test for a number of bases yet are composite, including one by Jaeschke which tests 'prime' on the 'Axiom' computer algebra system. These numbers are analysed in detail; a number of modifications to Rabin's test are proposed which together detect pseudoprimes constructed by all known means.

B Dixon, AK Lenstra, *Eurocrypt 92*
'Massively Parallel Elliptic Curve Factoring'

The elliptic curve factorisation algorithm is very suitable for parallel implementation, as it consists of many independent attempts to find a smooth number close to the desired prime factor. Using a 16K MasPar, a 40-digit prime factor of the 11279th partition number. Various optimisations were used and are described. The experience suggests that 50-digit primes will eventually be found using this technology, but 60-digit primes may well remain beyond reach of this algorithm.

DM Gordon, *Crypto 92*
'Designing and Detecting Trapdoors for Discrete Log Cryptosystems'

The number field seive can find discrete logarithms modulo any prime which can be expressed as a low degree polynomial with low coefficients of a small variable. A brief overview of the algorithm is presented, together with work estimates. It turns out that the optimal degree of the polynomial is four, and some 512 bit primes are not safe. However, a randomly chosen prime of this size is almost certain to be safe.

DM Gordon, KS McCurley, *Crypto 92*
'Massively Parallel Computation of Discrete Logarithms'

This extends to parallel machines the work of Coppersmith and Davenport on using index calculus to find logarithms in fields of characteristic two. Various techniques were used to speed up the algorithm and adapt it for parallel running. Smoothness testing was done by observing that polynomials over GF(2) of degree less than d can be seen as the vertices of a d-dimensional hypercube and searched efficiently using a Gray code. The resulting matrices were solved by the LaMacchia-Odlyzko method. The numerical results indicate that logarithms in GF(2^n) can be calculated now for $n = 521$, and $n = 593$ should be feasible in a few years.

A Granville, *Notices of the AMS v 39 no 7 pp 696 - 700*
'Primality Testing and Carmichael Numbers'

This is an introductory article, which describes the development of primality testing through the Chinese and Fermat, the discovery of Carmichael numbers, Korsolt's criterion, the Erdős construction, and the Alford variant of this. The climax is a sketch of the proof of the recent Alford-Granville-Pomerance theorem that there are infinitely many Carmichael numbers, and in particular, that given any finite set of bases, there are infinitely many Carmichael numbers which are strong pseudoprimes to all these bases.

K Koyama, Y Tsuruoka, *Crypto 92*
'Speeding up Elliptic Cryptosystems Using a Signed Binary Window Method'

An algorithm is presented to speed up multiplication of a point on an elliptic curve by pre-computing and using addition chains. With a 512 bit operand, this is found to require 602.6 multiplications on average. If parallel processing is allowed, each curve addition can be done in three field multiplications.

R Heiman, *Eurocrypt 92 rump session*
'Discrete Logs with Special Structure'

Special structures such as low Hamming weight may be used to accelerate computation in discrete log based cryptosystems. However this may be unwise as one can apply Shanks' method to get a search space whose size is the square root of the size of the restricted domain.

K Iwamura, T Matsumoto, H Imai, *Eurocrypt 92*
'High Speed Implementation Methods for RSA Scheme'

Two designs are proposed for more efficient modular multiplication. One of them should achieve a silicon efficiency of 2bps/gate compared with a previous best of 1.6 bps/gate; the other is based on a systolic array and planned to achieve a throughput of 200Kbps.

HW Lenstra, *Bulletin (new series) of the AMS, v 26 no 2 pp 211 - 244*
'Algorithms in Algebraic Number Theory'

This is an expository article focussing on determining Galois groups, the integer rings of algebraic number fields and their unit and class groups. It discusses the interplay between theoretical advances and computational results, and for which problems there exist algorithms with good asymptotic behaviour.

W Meier, O Staffelbach, *Crypto 92*
'Efficient Multiplication on Certain Nonsupersingular Elliptic Curves'

An algorithm is presented for fast multiplication on anomalous elliptic curves over $GF(2^n)$, and in particular for $y^2+xy=x^3+x^2+1$. This uses a normal basis and expresses multiplication as a short linear combination of powers of the Frobenius map. Experimentally, multiplication reduces to about $n/2$ curve additions, which is three times faster than previous methods.

RA Molin, HC Williams, *Utilitas Mathematica v 41 pp 259 - 308*
'Computation of the Class Number of a Real Quadratic Field'

This article reviews class group computation techniques for a nonspecialist mathematical reader. It gives a brief history of algebraic number theory and an overview of the relevant number theoretic tools, including ideals, class groups, regular primes, characters, L-functions, and the extended Riemann hypothesis; it then describes cycle counting and analytic methods of calculating class numbers.

WT Penzhorn, *Proc. 1992 South African COMSIG, p 169 - 172*
'Fast algorithms for the Generation of Large Primes For The RSA Cryptosystem'

This paper reviews the Rabin primality test, and shows that almost half the odd numbers can be filtered out in advance by trial division.

R Peralta, *Crypto 92*
'A Quadratic Seive on the n-Dimensional Cube'

An improvement is proposed in the quadratic seive: choose a smooth number t such that the number N to be factored has 2^n square roots mod t^2. These can be considered as a hypercube, on which we can find a Hamiltonian path of integers (X_i, Y_i) such that $X_i^2 = Y_i \pmod{N}$, allowing a fast search for square roots of smooth numbers. The algorithm is expected to be faster than the multiple polynomial quadratic seive.

R Peralta, *Math.Comp. v 58 no 197 pp 433 - 440*
'On the distribution of quadratic residues and nonresidues modulo a prime number'

If $a_1, \ldots, a_t$ are distinct mod p and x is chosen at random in Z_p, then the quadratic characters of $y_i = x + a_i$ have a joint distribution which differs from random by no more than $t(3+\sqrt{p})/p$. This has implications for the complexity of finding nonresidues and for the likelihood of failure in such a search.

L Rónyai, *SIAM J. Discrete Mathematics v 5 no 3 pp 345 - 365*
'Galois groups and factoring polynomials over finite fields'

This paper relaxes the conditions on factoring polynomials quickly over a finite field (given the generalised Riemann hypothesis); if a polynomial with integer coefficients has a discriminant which is not divisible by p, then its irreducible factors mod p can be found in polytime.

J Sauerbrey, A Dietel, *Eurocrypt 92*
'Resource Requirements for the Application of Addition Chains in Modulo Exponentiation'

Theoretical and simulation results are presented for the performance of addition chains in accelerating modular multiplication by randomly chosen exponents. A time/space compromise can be found by suitable selection of window sizes.

R Shawe-Taylor, *Electronics Letters v 28 no 2 pp 135 - 137*
'Proportion of primes generated by strong prime methods'

Formulae and numerical estimates are given for the number of primes generated by the Gordon and Shawe-Taylor methods. For example, of about 6.53 x 10^{74} 256-bit primes, the two methods generate 8.77 x 10^{-3} and 6.18 x 10^{-16} respectively.

V Shoup, *Math. Comp. v 58 no 197 pp 369 - 380*
'Searching for primitive roots in finite fields'

By testing all irreducible polynomials in sequence, one can reduce the problem of finding primitive polynomials in time $np^{O(1)}$ to testing for primitivity. If the extended Riemann hypothesis holds, two further results apply: there exists a deterministic search algorithm for primitive roots in GF(p^2), and the least primitive root mod p is O($r^4(\log r + 1)^4(\log p)^2$), where r is the number of distinct prime divisors of $p - 1$.

N Takagi, S Yajima. *IEEE Transactions on Computers v 41 no7 pp 887 - 891*
'Modular Multiplication Hardware Algorithms with a Redundant Representation and their Application to RSA'

A method is presented for speeding up modular arithmetic by using redundant representations of numbers to avoid carry propagation delays. The effect is that modular reduction involves examining only the three most significant symbols of each sum.

9 Secret Sharing

T Hwang, *Info. Processing Letters, v 42 no 4, pp 179 - 182*
'Protocols for group oriented secret sharing'

This proposal combines Diffie-Hellman key distribution with the Shamir secret sharing scheme to give a message broadcast protocol. This has the property that a message can be sent to a number of recipients, and any N of them can decipher it without the need for a trusted device. This is achieved by taking N shadows of a message key and combining them, using the Chinese Remainder Theorem.

T Kiesler, L Harn, *IEE Proc. Computers and Digital Techniques, v 139 no 3 pp 203 - 6*
'Cryptographic master-key generation scheme and its application to key distribution'

A variant on the Akl-Taylor-McKinnon-Meijer scheme is presented which accommodates hierarchies of master keys. It uses combinatorial products of the powers of a primitive root with respect to a modulus whose factorisation is known to the issuing authority.

F Piper, P Wild, *Discrete Mathematics v 106 pp 383 - 389*
'Incidence structures applied to cryptography'

This paper gives a general introduction to the use of combinatorial constructs in cryptography, particularly in key distribution patterns and secret sharing schemes. Combinatorial designs in particular can be used to prevent successful collusion by less than a given number of scheme members.

PD Seymour, *J. Comb. Theory series B v 56 pp 69 - 73*
'On Secret Sharing Matroids'

Secret sharing matroids are discussed. It had been conjectured that all matroids have the secret sharing property; it is shown that the Vamos matroid does not.

10 Complexity and Zero Knowledge

M Burmester, Y Desmedt, T Beth, *Computer Journal v 35 no 1 pp 21 - 29*
'Efficient Zero-Knowldge Identification Schemes for Smart Cards'

This paper proposes a zero-knowledge identification scheme in which the number of rounds is almost constant. The core of the scheme is a public value I and a secret s such that $I\beta^s \equiv 1 \pmod p$; in each round the prover chooses a random r and sends the verifier $z = \beta^r \pmod p$; she returns a random q; the prover supplies $y \equiv r + qs \pmod{(p-1)}$ and the verifier checks that $z \equiv \beta^y I^q \pmod p$. The scheme is then generalised to families of random homomorphisms.

M Burmester, *Info. Processing Letters v 42 no 2 pp 81 - 88*
'An almost constant-round interactive zero-knowledge proof'

This paper proposes a zero-knowledge identification scheme in which the number of rounds is almost constant. The scheme is a generalisation of the scheme presented in the above abstract.

A De Santis, G Persiano, *Proc. STACS 92 pp 439 - 448*
'Communication Efficient Zer-Knowledge Proofs of Knowledge (With Application to Electronic Cash)

A technique is shown whereby one can give any number of noninteractive zero- knowledge proofs for any NP language, on the assumption that one-way functions and suitable proofs of language membership exist. The practical value of the technique is that no trusted centre is needed and most transactions require just one round.

O Goldreich, H Krawczyk, *Random Structures and Algorithms v 3 no 2 pp 163 - 174*
'Sparse Pseudorandom Distributions'

The authors define these and prove their existence; they can be generated by probabilistic algorithms which expand short random strings into long pseudorandom ones. However sparse pseudorandom distributions exist which cannot be generated by a polytime algorithm, and this leads to the definition of evasive pseudorandom distributions as those such that no efficient algorithm will find strings of nonzero elements in them except with negligible probability.

J Goldstine, H Leung, D Wotschke, *Information and Computation v 100 no 2 pp 261 - 270*
'On the Relation between Ambiguity and Nondeterminism in Finite Automata'

Sublinear automata are defined as finite automata whose consumption of nondeterminism tends to infinity at a sublinear rate. The paper shows that these exist and that they have an infinite degree of ambiguity. Automata whose consumption of nondeterminism is bounded or linear can have any degree of ambiguity.

J Hartmannis, *Mitteilungen der mathematischen gesellschaft in Hamburg v 12 no 4 pp 961 - 975*
'On the structure of feasible computations'

This article reviews recent work in complexity theory from the standpoint of understanding why mathematics is difficult. In particular, theorem proving is NP complete; and NP = PSPACE if and only if in predicate calculus the length of proofs is polynomially bounded in their breadth. It also discusses IP = PSPACE and sketches the proof.

DH Johnson, *J. of Algorithms v 13 no 3 pp 502 - 524*
'The NP-Completeness Column: An Ongoing Guide'

This article reviews progress in complexity theory during the period 1988 to early 1992. Three advances are especially significant: the result IP = PSPACE of Shamir, Lund and others; unpublished recent work by Arora and others that NP = PCP[log(n),1] (NP complete problems are precisely those with probabilistically checkable proofs which use log(n) random bits and constant proof bits); and the link this gives to approximation theory by way of the NP completeness of the approximating clique problem.

E Kushilevitz, *SIAM J. Discrete Mathematics v 5 no 2 pp 273 - 284*
'Privacy and Communications Complexity'

A function is privately computable if and only if its matrix does not contain certain forbidden submatrices. from this it follows that the communication costs of private computation can be exponentially higher than those of non private computation; and in fact there is a dense hierarchy: for every positive function g(n) which grows no faster than $2(2^n - 1)$, there exists a function which is privately computable in g(n) rounds ,but not in g(n)-1.

UM Maurer, *Eurocrypt 92*
'Factoring with an Oracle'

The paper presents a much more efficient way to use an oracle to assist factoring. The idea is to ask for the index of the first elliptic curve to factor N. For all positive ϵ, this technique requires at most $\epsilon logN$ questions for large enough N.

T Okamoto, K Sakurai, H Shizuya, *Eurocrypt 92*
'How intractable is the Discrete Logarithm Problem for a General Finite Group?'

Provided that a general finite group G is in NP $\cap$ co-NP and its group operation can be performed in time polynomial in the element size, then the general discrete logarithm problem for G is in NP $\cap$ co-AM.

R Ostrovsky, R Venkatesan, M Yung, *Proc. STACS 92 pp 449 -460*
'Secure Commitment Against A Powerful Adversary'

This paper considers the feasibility of bit commitment where one of the parties has a computational advantage. It turns out that we can base suitable schemes on any averagely hard problem.

AL Seman, *Math. Systems Theory v 25 pp 203 - 221*
'A Survey of One-Way Functions in Complexity Theory'

One-way functions are characterised in various ways and their relationship to isomorphism and recognition problems in set theory is discussed, as are the implications for cryptography.