Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

293

Carl Pomerance (Ed.)

Advances in Cryptology — CRYPTO '87

Proceedings

Springer-Verlag

Lecture Notes in Computer Science

Edited by G. Goos and J. Hartmanis

293

Carl Pomerance (Ed.)

Advances in Cryptology — CRYPTO '87

Proceedings

Springer-Verlag
Berlin Heidelberg New York London Paris Tokyo

Editor

Carl Pomerance
Department of Mathematics, The University of Georgia
Athens, Georgia 30602, USA

CR Subject Classification (1987): E.3

ISBN 3-540-18796-0 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-18796-0 Springer-Verlag New York Berlin Heidelberg

Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
2145/3140-543210

Lecture Notes in Computer Science

Vol. 192: Automata on Infinite Words. Proceedings, 1984. Edited by M. Nivat and D. Perrin. V, 216 pages.1985.

Vol. 193: Logics of Programs. Proceedings, 1985. Edited by R. Parikh. VI, 424 pages. 1985.

Vol. 194: Automata, Languages and Programming. Proceedings, 1985. Edited by W. Brauer. IX, 520 pages. 1985.

Vol. 195: H. J. Stüttgen, A Hierarchical Associative Processing System. XII, 273 pages. 1985.

Vol. 196: Advances in Cryptology. Proceedings of CRYPTO '84. Edited by G.R. Blakley and D. Chaum. IX, 491 pages.1985.

Vol. 197: Seminar on Concurrency. Proceedings, 1984. Edited by S.D. Brookes, A. W. Roscoe and G. Winskel. X, 523 pages. 1985.

Vol. 198: A. Businger, PORTAL Language Description. VIII, 186 pages. 1985.

Vol. 199: Fundamentals of Computation Theory. Proceedings, 1985. Edited by L. Budach. XII, 533 pages. 1985.

Vol. 200: J.L.A. van de Snepscheut, Trace Theory and VLSI Design. VI, 0–140 pages. 1985.

Vol. 201: Functional Programming Languages and Computer Architecture. Proceedings, 1985. Edited by J.-P. Jouannaud. VI, 413 pages. 1985.

Vol. 202: Rewriting Techniques and Applications. Edited by J.-P. Jouannaud. VI, 441 pages. 1985.

Vol. 203: EUROCAL '85. Proceedings Vol. 1, 1985. Edited by B. Buchberger. V, 233 pages. 1985.

Vol. 204: EUROCAL '85. Proceedings Vol. 2, 1985. Edited by B. F. Caviness. XVI, 650 pages. 1985.

Vol. 205: P. Klint, A Study in String Processing Languages. VIII, 165 pages. 1985.

Vol. 206: Foundations of Software Technology and Theoretical Computer Science. Proceedings, 1985. Edited by S.N. Maheshwari. IX, 522 pages. 1985.

Vol. 207: The Analysis of Concurrent Systems. Proceedings, 1983. Edited by B.T. Denvir, W.T. Harwood, M.I. Jackson and M.J. Wray. VII, 398 pages. 1985.

Vol. 208: Computation Theory. Proceedings, 1984. Edited by A. Skowron. VII, 397 pages. 1985.

Vol. 209: Advances in Cryptology. Proceedings of EUROCRYPT '84. Edited by T. Beth, N. Cot and I. Ingemarsson. VII, 491 pages. 1985.

Vol. 210: STACS 86. Proceedings, 1986. Edited by B. Monien and G. Vidal-Naquet. IX, 368 pages. 1986.

Vol. 211: U. Schöning, Complexity and Structure. V, 99 pages. 1986.

Vol. 212: Interval Mathematics 1985. Proceedings, 1985. Edited by K. Nickel. VI, 227 pages. 1986.

Vol. 213: ESOP 86. Proceedings, 1986. Edited by B. Robinet and R. Wilhelm. VI, 374 pages. 1986.

Vol. 214: CAAP '86. 11th Colloquium on Trees in Algebra and Programming. Proceedings, 1986. Edited by P. Franchi-Zannettacci. VI, 306 pages. 1986.

Vol. 215: Mathematical Methods of Specification and Synthesis of Software Systems '85. Proceedings, 1985. Edited by W. Bibel and K.P. Jantke. 245 pages. 1986.

Vol. 216: Ch. Fernstrom, I. Kruzela, B. Svensson, LUCAS Associative Array Processor: Design, Programming and Application Studies. XII, 323 pages. 1986.

Vol. 217: Programs as Data Objects. Proceedings, 1985. Edited by H. Ganzinger and N.D. Jones. X, 324 pages. 1986.

Vol. 218: Advances in Cryptology – CRYPTO '85. Proceedings, 1985. Edited by H.C. Williams. X, 548 pages. 1986.

Vol. 219: Advances in Cryptology – EUROCRYPT '85. Proceedings, 1985. Edited by F. Pichler. IX, 281 pages. 1986.

Vol. 220: RIMS Symposia on Software Science and Engineering II. Proceedings, 1983 and 1984. Edited by E. Goto, K. Araki and T. Yuasa. XI, 323 pages. 1986.

Vol. 221: Logic Programming '85. Proceedings, 1985. Edited by E. Wada. IX, 311 pages. 1986.

Vol. 222: Advances in Petri Nets 1985. Edited by G. Rozenberg. VI, 498 pages. 1986.

Vol. 223: Structure in Complexity Theory. Proceedings, 1986. Edited by A.L. Selman. VI, 401 pages. 1986.

Vol. 224: Current Trends in Concurrency. Overviews and Tutorials. Edited by J.W. de Bakker, W.-P. de Roever and G. Rozenberg. XII, 716 pages. 1986.

Vol. 225: Third International Conference on Logic Programming. Proceedings, 1986. Edited by E. Shapiro. IX, 720 pages. 1986.

Vol. 226: Automata, Languages and Programming. Proceedings, 1986. Edited by L. Kott. IX, 474 pages. 1986.

Vol. 227: VLSI Algorithms and Architectures – AWOC 86. Proceedings, 1986. Edited by F. Makedon, K. Mehlhorn, T. Papatheodorou and P. Spirakis. VIII, 328 pages. 1986.

Vol. 228: Applied Algebra, Algorithmics and Error-Correcting Codes. AAECC-2. Proceedings, 1984. Edited by A. Poli. VI, 265 pages. 1986.

Vol. 229: Algebraic Algorithms and Error-Correcting Codes. AAECC-3. Proceedings, 1985. Edited by J. Calmet. VII, 416 pages. 1986.

Vol. 230: 8th International Conference on Automated Deduction. Proceedings, 1986. Edited by J.H. Siekmann. X, 708 pages. 1986.

Vol. 231: R. Hausser, NEWCAT: Parsing Natural Language Using Left-Associative Grammar. II, 540 pages. 1986.

Vol. 232: Fundamentals of Artificial Intelligence. Edited by W. Bibel and Ph. Jorrand. VII, 313 pages. 1986.

Vol. 233: Mathematical Foundations of Computer Science 1986. Proceedings, 1986. Edited by J. Gruska, B. Rovan and J. Wiedermann. IX, 650 pages. 1986.

Vol. 234: Concepts in User Interfaces: A Reference Model for Command and Response Languages. By Members of IFIP Working Group 2.7. Edited by D. Beech. X, 116 pages. 1986.

Vol. 235: Accurate Scientific Computations. Proceedings, 1985. Edited by W.L. Miranker and R.A. Toupin. XIII, 205 pages. 1986.

Vol. 236: TEX for Scientific Documentation. Proceedings, 1986. Edited by J. Désarménien. VI, 204 pages. 1986.

Vol. 237: CONPAR 86. Proceedings, 1986. Edited by W. Händler, D. Haupt, R. Jeltsch, W. Juling and O. Lange. X, 418 pages. 1986.

Vol. 238: L. Naish, Negation and Control in Prolog. IX, 119 pages. 1986.

Vol. 239: Mathematical Foundations of Programming Semantics. Proceedings, 1985. Edited by A. Melton. VI, 395 pages. 1986.

Vol. 240: Category Theory and Computer Programming. Proceedings, 1985. Edited by D. Pitt, S. Abramsky, A. Poigné and D. Rydeheard. VII, 519 pages. 1986.

Vol. 241: Foundations of Software Technology and Theoretical Computer Science. Proceedings, 1986. Edited by K.V. Nori. XII, 519 pages. 1986.

Vol. 242: Combinators and Functional Programming Languages. Proceedings, 1985. Edited by G. Cousineau, P.-L. Curien and B. Robinet. V, 208 pages. 1986.

Vol. 243: ICDT '86. Proceedings, 1986. Edited by G. Ausiello and P. Atzeni. VI, 444 pages. 1986.

Vol. 244: Advanced Programming Environments. Proceedings, 1986. Edited by R. Conradi, T.M. Didriksen and D.H. Wanvik. VII, 604 pages. 1986

CRYPTO'87

A Conference on the Theory and Applications of Cryptographic Techniques

held at the University of California, Santa Barbara,
through the cooperation of the
Computer Science Department

August 16-20, 1987

sponsored by:

The International Association for Cryptologic Research

in cooperation with

The IEEE Computer Society Technical Committee
On Security and Privacy

ORGANIZERS

General Chairman:	G. B. Agnew (U. Waterloo)
Program Committee:	T. A. Berson (Anagram Laboratories)
	E. F. Brickell (Bell Communications Research)
	A. M. Odlyzko (AT&T Bell Laboratories)
	C. Pomerance (U. Georgia, Chairman)
	G. J. Simmons (Sandia National Laboratories)

Preface

This book is the proceedings of CRYPTO'87, one in a series of annual conferences devoted to cryptologic research. For citations of proceedings of CRYPTO and Eurocrypt conferences before 1986, see

> Advances in Cryptology-CRYPTO'86 Proceedings, A. M. Odlyzko, ed., Lecture Notes in Computer Science #263, Springer, 1987.

Papers in this volume are organized into seven sections. The first six sections comprise all of the papers on the regular program, including two papers on the program that unfortunately were not presented at the meeting. The seventh section contains some of the papers presented at the "Rump Session" organized by W. Diffie and also includes a short note by T. R. N. Rao which comments on the paper of R. Struik and J. van Tilburg.

CRYPTO'87 was attended by 170 people representing 19 countries. Responsible not only for the conference as a whole, G. B. Agnew also took care of local arrangements in Santa Barbara. We all owe him a debt of gratitude for his highly successful efforts.

It is my special pleasure to thank my fellow members of the Program Committee: T. A. Berson, E. F. Brickell, A. M. Odlyzko, and G. J. Simmons. They all were most prompt, efficient, and willing to cheerfully compromise on disagreements. My task would have been hopeless without them.

I also would like to thank the authors and attendees who made CRYPTO'87 such a success. Special thanks are due to University of Georgia secretaries D. Byrd and P. Sisk and L. B. Montz at Springer for their help in the production of this volume.

Athens, Georgia

Carl Pomerance

Vol. 245: H.F. de Groote, Lectures on the Complexity of Bilinear Problems. V, 135 pages. 1987.

Vol. 246: Graph-Theoretic Concepts in Computer Science. Proceedings, 1986. Edited by G. Tinhofer and G. Schmidt. VII, 307 pages. 1987.

Vol. 247: STACS 87. Proceedings, 1987. Edited by F.J. Brandenburg, G. Vidal-Naquet and M. Wirsing. X, 484 pages. 1987.

Vol. 248: Networking in Open Systems. Proceedings, 1986. Edited by G. Müller and R.P. Blanc. VI, 441 pages. 1987.

Vol. 249: TAPSOFT '87. Volume 1. Proceedings, 1987. Edited by H. Ehrig, R. Kowalski, G. Levi and U. Montanari. XIV, 289 pages. 1987.

Vol. 250: TAPSOFT '87. Volume 2. Proceedings, 1987. Edited by H. Ehrig, R. Kowalski, G. Levi and U. Montanari. XIV, 336 pages. 1987.

Vol. 251: V. Akman, Unobstructed Shortest Paths in Polyhedral Environments. VII, 103 pages. 1987.

Vol. 252: VDM '87. VDM – A Formal Method at Work. Proceedings, 1987. Edited by D. Bjørner, C.B. Jones, M. Mac an Airchinnigh and E.J. Neuhold. IX, 422 pages. 1987.

Vol. 253: J.D. Becker, I. Eisele (Eds.), WOPPLOT 86. Parallel Processing: Logic, Organization, and Technology. Proceedings, 1986. V, 226 pages. 1987.

Vol. 254: Petri Nets: Central Models and Their Properties. Advances in Petri Nets 1986, Part I. Proceedings, 1986. Edited by W. Brauer, W. Reisig and G. Rozenberg. X, 480 pages. 1987.

Vol. 255: Petri Nets: Applications and Relationships to Other Models of Concurrency. Advances in Petri Nets 1986, Part II. Proceedings, 1986. Edited by W. Brauer, W. Reisig and G. Rozenberg. X, 516 pages. 1987.

Vol. 256: Rewriting Techniques and Applications. Proceedings, 1987. Edited by P. Lescanne. VI, 285 pages. 1987.

Vol. 257: Database Machine Performance: Modeling Methodologies and Evaluation Strategies. Edited by F. Cesarini and S. Salza. X, 250 pages. 1987.

Vol. 258: PARLE, Parallel Architectures and Languages Europe. Volume I. Proceedings, 1987. Edited by J.W. de Bakker, A.J. Nijman and P.C. Treleaven. XII, 480 pages. 1987.

Vol. 259: PARLE, Parallel Architectures and Languages Europe. Volume II. Proceedings, 1987. Edited by J.W. de Bakker, A.J. Nijman and P.C. Treleaven. XII, 464 pages. 1987.

Vol. 260: D.C. Luckham, F.W. von Henke, B. Krieg-Brückner, O. Owe, ANNA, A Language for Annotating Ada Programs. V, 143 pages. 1987.

Vol. 261: J. Ch. Freytag, Translating Relational Queries into Iterative Programs. XI, 131 pages. 1987.

Vol. 262: A. Burns, A.M. Lister, A.J. Wellings, A Review of Ada Tasking. VIII, 141 pages. 1987.

Vol. 263: A.M. Odlyzko (Ed.), Advances in Cryptology – CRYPTO '86. Proceedings. XI, 489 pages. 1987.

Vol. 264: E. Wada (Ed.), Logic Programming '86. Proceedings, 1986. VI, 179 pages. 1987.

Vol. 265: K.P. Jantke (Ed.), Analogical and Inductive Inference. Proceedings, 1986. VI, 227 pages. 1987.

Vol. 266: G. Rozenberg (Ed.), Advances in Petri Nets 1987. VI, 451 pages. 1987.

Vol. 267: Th. Ottmann (Ed.), Automata, Languages and Programming. Proceedings, 1987. X, 565 pages. 1987.

Vol. 268: P.M. Pardalos, J.B. Rosen, Constrained Global Optimization: Algorithms and Applications. VII, 143 pages. 1987.

Vol. 269: A. Albrecht, H. Jung, K. Mehlhorn (Eds.), Parallel Algorithms and Architectures. Proceedings, 1987. Approx. 205 pages. 1987.

Vol. 270: E. Börger (Ed.), Computation Theory and Logic. IX, 442 pages. 1987.

Vol. 271: D. Snyers, A. Thayse, From Logic Design to Logic Programming. IV, 125 pages. 1987.

Vol. 272: P. Treleaven, M. Vanneschi (Eds.), Future Parallel Computers. Proceedings, 1986. V, 492 pages. 1987.

Vol. 273: J.S. Royer, A Connotational Theory of Program Structure. V, 186 pages. 1987.

Vol. 274: G. Kahn (Ed.), Functional Programming Languages and Computer Architecture. Proceedings. VI, 470 pages. 1987.

Vol. 275: A.N. Habermann, U. Montanari (Eds.), System Development and Ada. Proceedings, 1986. V, 305 pages. 1987.

Vol. 276: J. Bézivin, J.-M. Hullot, P. Cointe, H. Lieberman (Eds.), ECOOP '87. European Conference on Object-Oriented Programming. Proceedings. VI, 273 pages. 1987.

Vol. 277: B. Benninghofen, S. Kemmerich, M.M. Richter, Systems of Reductions. X, 265 pages. 1987.

Vol. 278: L. Budach, R.G. Bukharajev, O.B. Lupanov (Eds.), Fundamentals of Computation Theory. Proceedings, 1987. XIV, 505 pages. 1987.

Vol. 279: J.H. Fasel, R.M. Keller (Eds.), Graph Reduction. Proceedings, 1986. XVI, 450 pages. 1987.

Vol. 280: M. Venturini Zilli (Ed.), Mathematical Models for the Semantics of Parallelism. Proceedings, 1986. V, 231 pages. 1987.

Vol. 281: A. Kelemenová, J. Kelemen (Eds.), Trends, Techniques, and Problems in Theoretical Computer Science. Proceedings, 1986. VI, 213 pages. 1987.

Vol. 282: P. Gorny, M.J. Tauber (Eds.), Visualization in Programming. Proceedings, 1986. VII, 210 pages. 1987.

Vol. 283: D.H. Pitt, A. Poigné, D.E. Rydeheard (Eds.), Category Theory and Computer Science. Proceedings, 1987. V, 300 pages. 1987.

Vol. 284: A. Kündig, R.E. Bührer, J. Dähler (Eds.), Embedded Systems. Proceedings, 1986. V, 207 pages. 1987.

Vol. 285: C. Delgado Kloos, Semantics of Digital Circuits. IX, 124 pages. 1987.

Vol. 286: B. Bouchon, R.R. Yager (Eds.), Uncertainty in Knowledge-Based Systems. Proceedings, 1986. VII, 405 pages. 1987.

Vol. 287: K.V. Nori (Ed.), Foundations of Software Technology and Theoretical Computer Science. Proceedings, 1987. IX, 540 pages. 1987.

Vol. 288: A. Blikle, MetaSoft Primer. XIII, 140 pages. 1987.

Vol. 289: H.K. Nichols, D. Simpson (Eds.), ESEC '87. 1st European Software Engineering Conference. Proceedings, 1987. XII, 404 pages. 1987.

Vol. 290: T.X. Bui, Co-oP A Group Decision Support System for Cooperative Multiple Criteria Group Decision Making. XIII, 250 pages. 1987.

Vol. 291: H. Ehrig, M. Nagl, G. Rozenberg, A. Rosenfeld (Eds.), Graph-Grammars and Their Application to Computer Science. VIII, 609 pages. 1987.

Vol. 292: The Munich Project CIP. Volume II: The Program Transformation System CIP-S. By the CIP System Group. VIII, 522 pages. 1987.

Vol. 293: C. Pomerance (Ed.), Advances in Cryptology — CRYPTO '87. Proceedings. X, 463 pages. 1988.

TABLE OF CONTENTS

SECTION 1: COMMUNICATION NETWORKS AND STANDARDS

SECTION 2: PROTOCOLS

SECTION 3: KEY DISTRIBUTION SYSTEMS

SECTION 4: PUBLIC KEY SYSTEMS

SECTION 5: DESIGN AND ANALYSIS OF CRYPTOGRAPHIC SYSTEMS

SECTION 6: APPLICATIONS

SECTION 7: INFORMAL CONTRIBUTIONS

SECTION 1

COMMUNICATION NETWORKS AND STANDARDS

STANDARDS FOR DATA SECURITY - A CHANGE OF DIRECTION

Wyn L.Price
National Physical Laboratory
Teddington, Middlesex, UK

Standards for data security - the achievement of acceptable privacy and integrity in data communication and storage - have been in preparation for the last fourteen years, beginning with the US Data Encryption Standard (DES). The DES was adopted as a US federal standard (1) in 1977, followed by adoption as an ANSI standard (2) in 1981. Since 1980 work has been in progress to develop a corresponding International Standards Organisation (ISO) text. For most practical purposes the ISO text was identical with the ANSI text; the only significant departure was that the eight parity bits allocated to the key in the US standard were left unallocated in the ISO text. The responsible ISO body was at first Technical Committee 97 (information processing), Working Group 1, TC97/WG1, which was followed by Sub-Committee 20 (data cryptographic techniques) of TC97, TC97/SC20. In May 1986 a discussion, followed by a resolution, took place in TC97, meeting in Washington, as a result of which a reference was made to the central governing body of ISO on which all national member bodies are represented, ISO Council, to decide whether it was wise to proceed to publication of the ISO standard. The outcome of this reference was that ISO Council decided to abandon work on the DES as a potential international standard. The decision was taken very late in the process of preparing the standard text, publication had been imminent.

The chief argument advanced in favour of the decision was that adoption as a standard might encourage overdependence on the DES algorithm. It is well-known that the financial institutions (banks, building societies, savings and loan, etc.) make very widespread use of the algorithm and the value of their daily transactions protected by the algorithm must be very substantial. This offers a very attractive potential target for criminal cryptanalysts. It was evidently feared within ISO that publication of an ISO standard for data encipherment would increase the attractiveness of the target by influencing even more users to depend on the one algorithm.

No-one is seriously suggesting that the useful lifetime of the DES is already over, but it is felt that preparation must be made for that time when it is judged no longer safe for use in protecting transactions of significant value or sensitivity. Various interesting academic results have been obtained in research investigations of the DES (3,4,5), but none of the people or groups involved is yet seriously claiming that the DES is broken. No one is yet able to predict whether the algorithm will succumb first to an analytic attack or to an exhaustive search for a key.

In the US the wish to replace the DES with more appropriate algorithms has led to the establishment of the Commercial COMSEC Endorsement Program (CCEP). This was originally meant to cover two security classes, Type I solely for US federal use and Type II for US federal and domestic commercial use, with the DES being phased out after 1988. However, it seems that the US financial institutions have requested that the DES be continued for financial applications beyond this date; the American Bankers Association has let it be known that the request for extension of approval for the DES has been granted. Neither Type I nor Type II CCEP algorithms are to be exportable and cannot therefore ever be put forward as candidates for international standardisation, should this be considered again in the future; the algorithms wil not be published.

In ISO the approach is somewhat different. ISO has decided to adopt the principle of a register of encipherment algorithms as a means of encouraging some degree of diversification in choice of encipherment algorithms. Algorithms, published and unpublished, will be entered on the register. Unpublished algorithms may be represented by name, supplier(s), block size and key domain; possibly speeds of operation may be entered. Published algorithms may be represented by a reference to a full and formal description of the algorithm; it is quite conceivable that the DES itself will figure in the register. Suppliers of algorithms will be free to offer their algorithms to ISO for entry on the register. Such an entry, however, is unlikely to offer any indication of the strength of an unpublished algorithm; it will be a matter for exercise of user judgement in choosing an algorithm to decide whether an algorithm is suitable for the proposed use. The decision to set up the register was noted by SC20, meeting in Ottawa in April 1987; the first relevant action was to establish a work item which is aimed at setting down the rules under which the register will operate. It is hoped that the operational rules will become available sometime in 1988, though a formal starting date for the register has not yet been decided.

Until recently work was also in progress within ISO to prepare a standard text for the RSA public key cryptosystem; this was a simple statement of the algorithm, the text of an implementation in Pascal, some sample parameters and an indication of the rules to be applied in choosing key material. However, a recent decision within ISO is to discontinue all work on standards for data encipherment; the embargo on data encipherment standards is therefore extended beyond the DES and now embraces public key algorithms and all others. Working Group 2 of SC20 (SC20/WG2) had been preparing not only the text of an RSA standard but also a technical report surveying recent developments in work on public key cryptography (a first edition of this technical report was published some years ago); the secretariat of TC97 now advises that work on the parts of the technical report relating to encipherment algorithms should also be discontinued. Regarding the RSA algorithm, this too is now fairly widely used in protecting transaction processing. It therefore seems likely that it will be offered as a candidate entry on the algorithm register. There will then be a need for a definitive statement of the algorithm in a form to which reference can be made; the academic papers in which the idea was first disclosed and later discussed and elaborated are not suitable for this purpose. The form that the definitive statement will need to take - it cannot be a formal standard text - has yet to be worked out.

In view of the removal of all the work on encipherment standards one might wonder what was left for TC97/SC20 to do. In fact the work programme of this committee is now heavier and more extensive than it was prior to the recent decisions.

The work programme adopted in April 1987 concentrates on operation of the register of algorithms and on standards for data security applications, including modes of operation for data encipherment, enhancement of communication protocols with security capability and security management (including management of encipherment keys).

One of the early effects of the removal of the work on data encipherment standards was to hold up work on two other standards which were also in an advanced state of preparation. These were respectively for 64 bit block cipher modes of operation and for enhancement of the physical layer of OSI (Open Systems Interconnection) with encipherment capability. The modes of operation document needed little doing to it to take into account the decision not to publish the DES standard text; this was because the modes of operation text had already been deliberately written in a general way, so that it applied to all 64 bit block ciphers and not just the DES. A little more effort was needed to change the physical layer standard. Publication of the 64 bit block modes of operation standard can be expected without undue further delay. Advancement of the physical layer text to Draft International Standard may also take place soon.

Work is in hand to prepare a standard for modes of operation of a block cipher not restricted to 64 bit blocks; this should present little difficulty, using the 64 bit block text as a basis. Any work on security enhancement at the link layer of OSI is now in abeyance because it was agreed that the demand for a standard in this context has not been established. The need for security enhancement at three other layers of OSI, namely network (layer 3), transport (layer 4) and presentation (layer 6) is recognised and work is now going ahead to prepare standard texts for these functions; the words of the respective work items specify 'conditions for the practical operation of cryptographic protection' at the various layers. Also in the context of secure communications architecture we have a new work item on 'practical conditions for the Associated Control Service Element (ACSE) authentication'.

In the area of key management the work programme is now more detailed; separate items on management of keys for secret key algorithms using secret key techniques, for management of keys for secret key algorithms using public key techniques and for management of keys for public key algorithms using public key techniques have been established. A further work item is to define a register of public keys and its functionality (not to be confused with the register of algorithms); the public key register is a service which will be required for many practical implementations of public key cryptography.

Peer entity authentication has a prominent place in the work programme. Texts are being circulated for draft proposal voting on a method for peer entity authentication using secret key algorithms and for two methods using public keys with two- and three-way handshakes. Work