LNCS 3348

Anne Canteaut
Kapaleeswaran Viswanathan (Eds.)

Progress in Cryptology – INDOCRYPT 2004

5th International Conference on Cryptology in India
Chennai, India, December 2004
Proceedings

Springer

Anne Canteaut
Kapaleeswaran Viswanathan (Eds.)

Progress in Cryptology – INDOCRYPT 2004

5th International Conference on Cryptology in India
Chennai, India, December 20-22, 2004
Proceedings

Springer

Volume Editors

Anne Canteaut
Institut National de Recherche en Informatique et Automatique (INRIA)
Projet CODES, Domaine de Voluceau, Rocquencourt
78153 Le Chesnay Cedex, France
E-mail: anne.canteaut@inria.fr

Kapaleeswaran Viswanathan
SETS, 21 Mangadu Swamy Street, Nungambakkam
Chennai 600 034, India
E-mail: kapali@sets.org.in

Library of Congress Control Number: 2004116723

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, F.2.1, C.2

ISSN 0302-9743
ISBN 3-540-24130-2 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11369165 06/3142 5 4 3 2 1 0

Preface

The INDOCRYPT series of conferences started in 2000. INDOCRYPT 2004 was the fifth one in this series. The popularity of this series is increasing every year. The number of papers submitted to INDOCRYPT 2004 was 181, out of which 147 papers conformed to the specifications in the call for papers and, therefore, were accepted to the review process. Those 147 submissions were spread over 22 countries.

Only 30 papers were accepted to this proceedings. We should note that many of the papers that were not accepted were of good quality but only the top 30 papers were accepted. Each submission received at least three independent reviews. The selection process also included a Web-based discussion phase. We made efforts to compare the submissions with other ongoing conferences around the world in order to ensure detection of double-submissions, which were not allowed by the call for papers. We wish to acknowledge the use of the Web-based review software developed by Bart Preneel, Wim Moreau, and Joris Claessens in conducting the review process electronically. The software greatly facilitated the Program Committee in completing the review process on time. We would like to thank Cédric Lauradoux and the team at INRIA for their total support in configuring and managing the Web-based submission and review softwares. We are unable to imagine the outcome of the review process without their participation.

This year the invited talks were presented by Prof. Colin Boyd and Prof. Amit Sahai. Colin provided a talk on the design of key establishment protocols while Amit presented a talk on secure protocols for complex tasks in complex environments. They presented two sides of the same coin so that the audience can gain a more comprehensive view of the analysis and design of cryptographic protocols. We hope that the invited talks contributed their share to promoting such an exciting area in cryptology research in India. At the same time, the invited talks were of great value for international researchers, as well, because Colin and Amit shared the latest results of their research activities.

The smooth and successful progress of INDOCRYPT 2004 was due to the efforts of many individuals. The members of the Program Committee worked hard throughout, and did an excellent job. Many external reviewers contributed their time and expertise to aid our decision-making. The Organizing Committee put its maximal effort into ensuring the successful progress of this conference. We wish to thank Prof. R. Balasubramaniam and Dr. M.S. Vijayaraghavan for being the general co-chairs of this conference. We also thank the Cryptology Research Society of India and ISI, Calcutta.

We hope that the INDOCRYPT series of conferences remains a forum for discussing high-quality results in the area of cryptology and its applications to information security in the years to come.

December 2004

Anne Canteaut
Kapaleeswaran Viswanathan

Organization

The INDOCRYPT Conferences are the annual events of the Cryptology Research Society of India. INDOCRYPT 2004 was organized by IMSc, Chennai, and SETS, Chennai.

General Co-chairs

R. Balasubramanian	Institute for Mathematical Sciences, India
M.S. Vijayaraghavan	SETS, India

Program Co-chairs

Anne Canteaut	INRIA, France
Kapaleeswaran Viswanathan	SETS, India

Program Committee

Michael Backes	IBM, Zurich, Switzerland
Colin Boyd	Queensland University of Technology, Australia
Anne Canteaut	INRIA, France
Cunsheng Ding	Hong Kong University of Science and Technology, China
Andreas Enge	Ecole Polytechnique, France
Caroline Fontaine	CNRS, France
Henri Gilbert	France Telecom R&D, France
Juanma Gonzalez-Nieto	Queensland University of Technology, Australia
Tor Helleseth	University of Bergen, Norway
Thomas Johansson	Lund University, Sweden
Kwangjo Kim	Information and Communications University, Korea
Tanja Lange	University of Bochum, Germany
Arjen Lenstra	Lucent Technologies, USA and Technische Universiteit Eindhoven, The Netherlands
C.E. Veni Madhavan	Indian Institute of Science, Bangalore, India
Keith Martin	Royal Holloway University of London, UK
Anish Mathuria	Dhirubhai Ambani, Institute of Information and Communication Technology, India

Alfred Menezes	University of Waterloo, Canada
Shiho Moriai	Sony Computer Entertainment Inc., Japan
Kenneth Paterson	Royal Holloway University of London, UK
Kapil H. Paranjape	IMSc, Chennai, India
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Bimal Roy	ISI Kolkata, India
Amit Sahai	Princeton University, USA
Palash Sarkar	ISI Kolkata, India
Henk van Tilborg	Technische Universiteit Eindhoven, The Netherlands
D.G. Thomas	Madras Christian College, India
Kapaleeswaran Viswanathan	SETS, Chennai, India
Adam Young	Cigital Labs, USA
Moti Yung	Columbia University, USA

Organizing Committee

Dr. A.K. Chakravarthy	Dept. of IT, MICT, Govt. of India
Mr. Cédric Lauradoux	INRIA, France
Dr. K. Srinivas	IMSc, India
Dr. N.Vijayarangan	SETS, India

Organizing Sub-committee

Mr. G. Aswin	SETS, India
Mr. C. Stephen Balasundaram	SETS, India
Mr. Manish Chauhan	SETS, India
Ms. R. Indra	IMSc, India
Ms. K. Jayasri	SETS, India
Mr. R. Harish Kumar	SETS, India
Mr. Ramakrishna Manja	IMSc, India
Dr. Paul Pandian	IMSc, India
Mr. Vishnu Prasath	IMSc, India
Ms. A. Suganya	SETS, India
Mr. R. Vijayasarathy	SETS, India

External Referees

P.J. Abisha
Avishek Adhikari
Riza Aditya
Toru Akishita
Sattam Al-Riyami
Lejla Batina
Côme Berbain
Thierry Berger
Florent Bersani
Alex Biryukov
Simon Blackburn
Emmanuel Bresson

Jan Camenisch
Liqun Chen
Olivier Chevassut
Matthijs Coster
Deepak Kumar Dalai
V. Rajkumar Dare
Christophe De Cannière
Alex Dent
Jeroen Doumen
Dang Nguyen Duc
Sylvain Duquesne
Håkan Englund
Steven Galbraith
Pierrick Gaudry
Daniel Gottesman
Robert Granger
Kishan Chand Gupta
Darrel Hankerson
Guillaume Hanrot
Martin Hell
Clemens Heuberger
Shoichi Hirose
Yvonne Hitchcock
Dennis Hofheinz
Tetsu Iwata
Cees Jansen
Ellen Jochemsz
Stefan Katzenbeisser
Alexander Kholosha
Caroline Kudla
Joseph Lano
Hyunrok Lee
Kerstin Lemke
Benoît Libert
Vo Duc Liem
Phil MacKenzie
John Malone-Lee
Alexander Maximov
Nele Mentens
Chris Mitchell
Suman K. Mitra
François Morain
Sumio Morioka
Joern Mueller-Quade
James Muir
Svetla Nikova
Luke O'Connor
Siddika Berna Ors
Daniel Page
Matthew Parker
Olivier Pereira
Håvard Raddum
Zulfikar Ramzan
K. Rangarajan
François Recher
Akashi Satoh
Werner Schindler
Takeshi Shimoyama
Taizo Shirai
Jamshid Shokrollahi
Hervé Sibert
Francesco Sica
Andrey Sidorenko
Martijn Stam
Tsuyoshi Takagi
Gerard Tel
Yuuki Tokunaga
Ludo Tolhuizen
Emmanuel Thomé
Pim Tuyls
M.K. Viswanath
Brent Waters
Benne de Weger
Annegret Weng
Arne Winterhof
Christopher Wolf
Robbie Ye
Feng Zhu

Sponsoring Institutions

Bharat Electronics Limited
BRNS Secretariat, Bhabha Atomic Research Centre
Department of Information Technology, Government of India
Department of Science and Technology, Government of India
Electronics Corporation of India Limited
Hewlett Packard India Private Limited
Institute for Development and Research in Banking Technology
NASSCOM
SLN Technologies Private Limited
Sun Microsystems India Private Limited

Lecture Notes in Computer Science

For information about Vols. 1–3245

please contact your bookseller or Springer

Vol. 3356: G. Das, V.P. Gulati (Eds.), Intelligent Information Technology. XII, 428 pages. 2004.

Vol. 3348: A. Canteaut, K. Viswanathan (Eds.), Progress in Cryptology - INDOCRYPT 2004. XIV, 431 pages. 2004.

Vol. 3347: R.K. Ghosh, H. Mohanty (Eds.), Distributed Computing and Internet Technology. XX, 472 pages. 2004.

Vol. 3341: R. Fleischer, G. Trippen (Eds.), Algorithms and Computation. XVII, 935 pages. 2004.

Vol. 3340: C.S. Calude, E. Calude, M.J. Dinneen (Eds.), Developments in Language Theory. XI, 431 pages. 2004.

Vol. 3339: G.I. Webb, X. Yu (Eds.), AI 2004: Advances in Artificial Intelligence. XXII, 1272 pages. 2004. (Subseries LNAI).

Vol. 3338: S.Z. Li, J. Lai, T. Tan, G. Feng, Y. Wang (Eds.), Advances in Biometric Person Authentication. XVIII, 699 pages. 2004.

Vol. 3337: J.M. Barreiro, F. Martin-Sanchez, V. Maojo, F. Sanz (Eds.), Biological and Medical Data Analysis. XI, 508 pages. 2004.

Vol. 3336: D. Karagiannis, U. Reimer (Eds.), Practical Aspects of Knowledge Management. X, 523 pages. 2004. (Subseries LNAI).

Vol. 3334: Z. Chen, H. Chen, Q. Miao, Y. Fu, E. Fox, E.-p. Lim (Eds.), Digital Libraries: International Collaboration and Cross-Fertilization. XX, 690 pages. 2004.

Vol. 3333: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part III. XXXV, 785 pages. 2004.

Vol. 3332: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part II. XXXVI, 1051 pages. 2004.

Vol. 3331: K. Aizawa, Y. Nakamura, S. Satoh (Eds.), Advances in Multimedia Information Processing - PCM 2004, Part I. XXXVI, 667 pages. 2004.

Vol. 3329: P.J. Lee (Ed.), Advances in Cryptology - ASIACRYPT 2004. XVI, 546 pages. 2004.

Vol. 3328: K. Lodaya, M. Mahajan (Eds.), FSTTCS 2004: Foundations of Software Technology and Theoretical Computer Science. XVI, 532 pages. 2004.

Vol. 3323: G. Antoniou, H. Boley (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 215 pages. 2004.

Vol. 3322: R. Klette, J. Žunić (Eds.), Combinatorial Image Analysis. XII, 760 pages. 2004.

Vol. 3321: M.J. Maher (Ed.), Advances in Computer Science - ASIAN 2004. XII, 510 pages. 2004.

Vol. 3321: M.J. Maher (Ed.), Advances in Computer Science - ASIAN 2004. XII, 510 pages. 2004.

Vol. 3320: K.-M. Liew, H. Shen, S. See, W. Cai (Eds.), Parallel and Distributed Computing: Applications and Technologies. XXIV, 891 pages. 2004.

Vol. 3316: N.R. Pal, N.K. Kasabov, R.K. Mudi, S. Pal, S.K. Parui (Eds.), Neural Information Processing. XXX, 1368 pages. 2004.

Vol. 3315: C. Lemaître, C.A. Reyes, J.A. González (Eds.), Advances in Artificial Intelligence – IBERAMIA 2004. XX, 987 pages. 2004. (Subseries LNAI).

Vol. 3314: J. Zhang, J.-H. He, Y. Fu (Eds.), Computational and Information Science. XXIV, 1259 pages. 2004.

Vol. 3312: A.J. Hu, A.K. Martin (Eds.), Formal Methods in Computer-Aided Design. XI, 445 pages. 2004.

Vol. 3311: V. Roca, F. Rousseau (Eds.), Interactive Multimedia and Next Generation Networks. XIII, 287 pages. 2004.

Vol. 3309: C.-H. Chi, K.-Y. Lam (Eds.), Content Computing. XII, 510 pages. 2004.

Vol. 3308: J. Davies, W. Schulte, M. Barnett (Eds.), Formal Methods and Software Engineering. XIII, 500 pages. 2004.

Vol. 3307: C. Bussler, S.-k. Hong, W. Jun, R. Kaschek, D.. Kinshuk, S. Krishnaswamy, S.W. Loke, D. Oberle, D. Richards, A. Sharma, Y. Sure, B. Thalheim (Eds.), Web Information Systems – WISE 2004 Workshops. XV, 277 pages. 2004.

Vol. 3306: X. Zhou, S. Su, M.P. Papazoglou, M.E. Orlowska, K.G. Jeffery (Eds.), Web Information Systems – WISE 2004. XVII, 745 pages. 2004.

Vol. 3305: P.M.A. Sloot, B. Chopard, A.G. Hoekstra (Eds.), Cellular Automata. XV, 883 pages. 2004.

Vol. 3303: J.A. López, E. Benfenati, W. Dubitzky (Eds.), Knowledge Exploration in Life Science Informatics. X, 249 pages. 2004. (Subseries LNAI).

Vol. 3302: W.-N. Chin (Ed.), Programming Languages and Systems. XIII, 453 pages. 2004.

Vol. 3299: F. Wang (Ed.), Automated Technology for Verification and Analysis. XII, 506 pages. 2004.

Vol. 3298: S.A. McIlraith, D. Plexousakis, F. van Harmelen (Eds.), The Semantic Web – ISWC 2004. XXI, 841 pages. 2004.

Vol. 3296: L. Bougé, V.K. Prasanna (Eds.), High Performance Computing - HiPC 2004. XXV, 530 pages. 2004.

Vol. 3295: P. Markopoulos, B. Eggen, E. Aarts, J.L. Crowley (Eds.), Ambient Intelligence. XIII, 388 pages. 2004.

Vol. 3294: C.N. Dean, R.T. Boute (Eds.), Teaching Formal Methods. X, 249 pages. 2004.

Vol. 3293: C.-H. Chi, M. van Steen, C. Wills (Eds.), Web Content Caching and Distribution. IX, 283 pages. 2004.

Vol. 3292: R. Meersman, Z. Tari, A. Corsaro (Eds.), On the Move to Meaningful Internet Systems 2004: OTM 2004 Workshops. XXIII, 885 pages. 2004.

Vol. 3291: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2004: CoopIS, DOA, and ODBASE, Part II. XXV, 824 pages. 2004.

Vol. 3290: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2004: CoopIS, DOA, and ODBASE, Part I. XXV, 823 pages. 2004.

Vol. 3289: S. Wang, K. Tanaka, S. Zhou, T.W. Ling, J. Guan, D. Yang, F. Grandi, E. Mangina, I.-Y. Song, H.C. Mayr (Eds.), Conceptual Modeling for Advanced Application Domains. XXII, 692 pages. 2004.

Vol. 3288: P. Atzeni, W. Chu, H. Lu, S. Zhou, T.W. Ling (Eds.), Conceptual Modeling – ER 2004. XXI, 869 pages. 2004.

Vol. 3287: A. Sanfeliu, J.F. Martínez Trinidad, J.A. Carrasco Ochoa (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XVII, 703 pages. 2004.

Vol. 3286: G. Karsai, E. Visser (Eds.), Generative Programming and Component Engineering. XIII, 491 pages. 2004.

Vol. 3285: S. Manandhar, J. Austin, U.B. Desai, Y. Oyanagi, A. Talukder (Eds.), Applied Computing. XII, 334 pages. 2004.

Vol. 3284: A. Karmouch, L. Korba, E.R.M. Madeira (Eds.), Mobility Aware Technologies and Applications. XII, 382 pages. 2004.

Vol. 3283: F.A. Aagesen, `C. Anutariya, V. Wuwongse (Eds.), Intelligence in Communication Systems. XIII, 327 pages. 2004.

Vol. 3282: V. Guruswami, List Decoding of Error-Correcting Codes. XIX, 350 pages. 2004.

Vol. 3281: T. Dingsøyr (Ed.), Software Process Improvement. X, 207 pages. 2004.

Vol. 3280: C. Aykanat, T. Dayar, İ. Körpeoğlu (Eds.), Computer and Information Sciences - ISCIS 2004. XVIII, 1009 pages. 2004.

Vol. 3278: A. Sahai, F. Wu (Eds.), Utility Computing. XI, 272 pages. 2004.

Vol. 3275: P. Perner (Ed.), Advances in Data Mining. VIII, 173 pages. 2004. (Subseries LNAI).

Vol. 3274: R. Guerraoui (Ed.), Distributed Computing. XIII, 465 pages. 2004.

Vol. 3273: T. Baar, A. Strohmeier, A. Moreira, S.J. Mellor (Eds.), <<UML>> 2004 - The Unified Modelling Language. XIII, 454 pages. 2004.

Vol. 3271: J. Vicente, D. Hutchison (Eds.), Management of Multimedia Networks and Services. XIII, 335 pages. 2004.

Vol. 3270: M. Jeckle, R. Kowalczyk, P. Braun (Eds.), Grid Services Engineering and Management. X, 165 pages. 2004.

Vol. 3269: J. Lopez, S. Qing, E. Okamoto (Eds.), Information and Communications Security. XI, 564 pages. 2004.

Vol. 3268: W. Lindner, M. Mesiti, C. Türker, Y. Tzitzikas, A. Vakali (Eds.), Current Trends in Database Technology - EDBT 2004 Workshops. XVIII, 608 pages. 2004.

Vol. 3267: C. Priami, P. Quaglia (Eds.), Global Computing. VIII, 377 pages. 2004.

Vol. 3266: J. Solé-Pareta, M. Smirnov, P.V. Mieghem, J. Domingo-Pascual, E. Monteiro, P. Reichl, B. Stiller, R.J. Gibbens (Eds.), Quality of Service in the Emerging Networking Panorama. XVI, 390 pages. 2004.

Vol. 3265: R.E. Frederking, K.B. Taylor (Eds.), Machine Translation: From Real Users to Research. XI, 392 pages. 2004. (Subseries LNAI).

Vol. 3264: G. Paliouras, Y. Sakakibara (Eds.), Grammatical Inference: Algorithms and Applications. XI, 291 pages. 2004. (Subseries LNAI).

Vol. 3263: M. Weske, P. Liggesmeyer (Eds.), Object-Oriented and Internet-Based Technologies. XII, 239 pages. 2004.

Vol. 3262: M.M. Freire, P. Chemouil, P. Lorenz, A. Gravey (Eds.), Universal Multiservice Networks. XIII, 556 pages. 2004.

Vol. 3261: T. Yakhno (Ed.), Advances in Information Systems. XIV, 617 pages. 2004.

Vol. 3260: I.G.M.M. Niemegeers, S.H. de Groot (Eds.), Personal Wireless Communications. XIV, 478 pages. 2004.

Vol. 3259: J. Dix, J. Leite (Eds.), Computational Logic in Multi-Agent Systems. XII, 251 pages. 2004. (Subseries LNAI).

Vol. 3258: M. Wallace (Ed.), Principles and Practice of Constraint Programming – CP 2004. XVII, 822 pages. 2004.

Vol. 3257: E. Motta, N.R. Shadbolt, A. Stutt, N. Gibbins (Eds.), Engineering Knowledge in the Age of the Semantic Web. XVII, 517 pages. 2004. (Subseries LNAI).

Vol. 3256: H. Ehrig, G. Engels, F. Parisi-Presicce, G. Rozenberg (Eds.), Graph Transformations. XII, 451 pages. 2004.

Vol. 3255: A. Benczúr, J. Demetrovics, G. Gottlob (Eds.), Advances in Databases and Information Systems. XI, 423 pages. 2004.

Vol. 3254: E. Macii, V. Paliouras, O. Koufopavlou (Eds.), Integrated Circuit and System Design. XVI, 910 pages. 2004.

Vol. 3253: Y. Lakhnech, S. Yovine (Eds.), Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems. X, 397 pages. 2004.

Vol. 3252: H. Jin, Y. Pan, N. Xiao, J. Sun (Eds.), Grid and Cooperative Computing - GCC 2004 Workshops. XVIII, 785 pages. 2004.

Vol. 3251: H. Jin, Y. Pan, N. Xiao, J. Sun (Eds.), Grid and Cooperative Computing - GCC 2004. XXII, 1025 pages. 2004.

Vol. 3250: L.-J. (LJ) Zhang, M. Jeckle (Eds.), Web Services. X, 301 pages. 2004.

Vol. 3249: B. Buchberger, J.A. Campbell (Eds.), Artificial Intelligence and Symbolic Computation. X, 285 pages. 2004. (Subseries LNAI).

Vol. 3247: D. Comaniciu, R. Mester, K. Kanatani, D. Suter (Eds.), Statistical Methods in Video Processing. VIII, 199 pages. 2004.

Vol. 3246: A. Apostolico, M. Melucci (Eds.), String Processing and Information Retrieval. XIV, 332 pages. 2004.

Table of Contents

Invited Talks

Cryptographic Protocols

Applications

Stream Ciphers

Cryptographic Boolean Functions

Foundations

Block Ciphers

Public Key Encryption

Efficient Representations

Public Key Cryptanalysis

Modes of Operation

Signatures

Traitor Tracing and Visual Cryptography

Design of Secure Key Establishment Protocols: Successes, Failures and Prospects

Colin Boyd*

Information Security Research Centre,
Queensland University of Technology,
Brisbane Q4001, Australia
boyd@isrc.qut.edu.au

Abstract. Key establishment protocols form one of the most basic types of cryptographic protocols and have been studied intensively for over 20 years. The current status of design and analysis methods is reviewed with particular reference to formal appoaches. Likely future trends and open issues are also discussed.

1 Introduction

Key establishment is a foundational element for secure communications. It concerns how to set up a new key (a *session key*) to protect communications during a subsequent session. In terms of modern cryptography it is a venerable problem that has been widely studied from almost every conceivable angle. One may ask how hard it can be to consider all ways of setting up a session key. Yet the evidence is that this study has not yet been exhaustive. One reason for this is that new requirements have become evident over time that were not previously recognised. Another reason is that there is no well-defined method to explore the space of possible secure protocols. Even until today most systematic or formal techniques allow only protocol analysis and not design of protocols to meet specific requirements. The purposes of this paper are:

- to explore current techniques to ensure the security of key establishment protocols, particularly those with some formal basis;
- to consider to what extent these methods can be used to systematically design new protocols;
- to summarise (and speculate on) prospects for the future of these methods.

In the rest of this introduction some background information is provided on protocol types and potential security requirements. Section 2 looks at informal design principles for key establishment. Sections 3 and 4 are devoted to the two main formal approaches to protocol analysis: the formal methods approach which

* Research funded by Australian Research Council under Discovery Project DP0345775.

A. Canteaut and K. Viswanathan (Eds.): INDOCRYPT 2004, LNCS 3348, pp. 1–13, 2004.

comes from the computer security research community, and the computational approach which comes from the cryptography research community. Section 5 discusses current trends and prospects for combining the benefits of both these approaches.

1.1 Key Agreement and Key Transport

A common way of classifying key establishment is to consider protocols which provide either *key agreement* or *key transport.* Key agreement protocols require input to the session key from both parties in a two-party protocol, or more generally from more than one party in a multi-party protocol. In a key transport protocol one party (often a trusted third party) chooses the key and forwards it to the other parties.

It is often stated that key agreement is preferable to key transport. Reasons given are that key agreement is 'fairer' since no party is able to fix the key value. However, this property does not correspond to any standard security property and most models do not in any case take account of malicious insiders. Since any party is free to give away the session key at will, what may be the benefit of making the key some fixed value? In addition, it is often suggested that using pseudo-random input from more than one party serves to increase the randomness of the final key. This may or may not be useful depending on how the values are combined. In particular, suppose that two parties A and B provide values g^x and g^y in the classic Diffie-Hellman key agreement protocol. If the random number generator of A is very weak then it may be easy for an adversary to obtain x and hence the shared key g^{xy}, no matter how strong is the random number generator of B[1].

1.2 Adding Requirements

One reason that key establishment continues to be a challenging problem is the addition of new properties that are desired in certain situations. These include ways of strengthening the security properties such as the following.

Forward Secrecy is the property that compromise of long-term keys should not compromise session keys that were previously accepted. Forward secrecy is increasingly regarded as a very desirable property. It seems to be achievable only through the use of ephemeral public keys, such as in Diffie-Hellman key exchange. (Although it is not widely recognised, ephemeral keys from any public key encryption scheme can be used to provide forward secrecy, including RSA as noted by Wiener [Wie98].)

Resistance to Key Compromise Impersonation is a less widely discussed property that is related to forward secrecy in that it concerns what may happen after long-term keys are compromised. It demands that the adversary who has obtained the long-term key of entity A is unable to masquerade as other principals to A.

[1] This observation was made to me by Carsten Rudolph.

Anonymity of Principals was often neglected in the past, but with the prevalence of communications on public (including wireless) networks it is more widely recognised as an issue. For example, the Internet Key Exchange (IKE) protocol [HC98] explicitly addresses this requirement, although its provision is not so robust as may have been initially expected [PK00].

Resistance to Denial of Service is a pressing practical need for protocols, particularly those run on open networks. This is another property that was considered in the design of IKE, although there has been much controversy over the resulting solution [PK00].

As well as the above extra security features that can be relevant to any security architecture, some protocols have extra fundamental assumptions about the way that the network is set up and the security infrastructure in place.

Group Key Establishment protocols have become very popular in the recent literature in line with the increase in collaborative communications applications. There are many possible types of architecture. One of the most challenging is the ad-hoc network where the security infrastructure may be minimal.

Low-Power Principals are as prevalent as ever, due to the inexorable miniaturisation of devices. The most common example has been the mobile telephone, and there are many protocols designed specifically for its use. New lightweight technologies, such as RFID tags, open up new challenges.

Password-Based Protocols were first introduced around 15 years ago. These protocols assume that shared keys have only a small amount of entropy, and must therefore be robust against off-line guessing attacks in which the adversary attempts to eliminate potential passwords using public information. Recently such protocols have attracted extensive interest, and standards in both IEEE [IEE04] and ISO are in preparation.

Identity-Based Protocols have been around for about 20 years but recent techniques based on elliptic curve pairings have resulted in an explosion of interest in this area. These protocols allow users to establish keys without the use of an on-line server or a public key infrastructure. There is likely to be continuing interest in this area and to date few key establishment protocols using the new techniques come with a proof of security.

Notice that most combinations of the above requirements or scenarios are possible, although some are in conflict with others. For example, protocols providing forward secrecy are typically more computationally expensive than those that do not. Therefore protocols designed for low-power principals often sacrifice forward secrecy for benefits in efficiency.

2 Design Principles

In 1994 Abadi and Needham gathered together the experience of many years and produced a set of 11 rules of thumb to be used as principles for designers of cryptographic protocols [AN94]. The following year Anderson and Needham