Anne Canteaut
Kapaleeswaran Viswanathan (Eds.)

Progress in Cryptology –
INDOCRYPT 2004

5th International Conference on Cryptology in India
Chennai, India, December 20-22, 2004
Proceedings
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
Sattam Al-Riyami
Florent Bersani

Avishek Adhikari
Lejla Batina
Alex Biryukov

Riza Aditya
Côme Berbain
Simon Blackburn

Toru Akishita
Thierry Berger
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
Pierick 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
# Table of Contents

## Invited Talks

Design of Secure Key Establishment Protocols: Successes, Failures and Prospects  
*Colin Boyd* ................................................... 1

Secure Protocols for Complex Tasks in Complex Environments  
*Amit Sahai* ................................................... 14

## Cryptographic Protocols

Tripartite Key Exchange in the Canetti-Krawczyk Proof Model  
*Yvonne Hitchcock, Colin Boyd, Juan Manuel González Nieto* ........ 17

The Marriage Proposals Problem: Fair and Efficient Solution for Two-Party Computations  
*Audrey Montreuil, Jacques Patarin* ............................. 33

## Applications

On the Security of a Certified E-Mail Scheme  
*Guilin Wang, Feng Bao, Jianying Zhou* .......................... 48

Multiplicative Homomorphic E-Voting  
*Kun Peng, Riza Aditya, Colin Boyd, Ed Dawson, Byoungcheon Lee* .............................................. 61

## Stream Ciphers

Chosen Ciphertext Attack on a New Class of Self-Synchronizing Stream Ciphers  
*Bin Zhang, Hongjun Wu, Dengguo Feng, Feng Bao* ............... 73

Algebraic Attacks Over $GF(q)$  
*Lynn Margaret Batten* ........................................... 84
## Table of Contents

### Cryptographic Boolean Functions

Results on Algebraic Immunity for Cryptographically Significant Boolean Functions

_Deepak Kumar Dalai, Kishan Chand Gupta, Subhamoy Maitra_  

... 92

Generalized Boolean Bent Functions

_Laurent Poinsot, Sami Harari_  

... 107

On Boolean Functions with Generalized Cryptographic Properties

_An Braeken, Ventzislav Nikov, Svetla Nikova, Bart Preneel_  

... 120

### Foundations

Information Theory and the Security of Binary Data Perturbation

_Poorvi L. Vora_  

... 136

Symmetric Authentication Codes with Secrecy and Unconditionally Secure Authenticated Encryption

_Luke McAven, Reihaneh Safavi-Naini, Moti Yung_  

... 148

### Block Ciphers

Faster Variants of the MESH Block Ciphers

_Jorge Nakahara Júnior_  

... 162

Related-Key Attacks on Reduced Rounds of SHACAL-2

_Jongsung Kim, Guil Kim, Sangjin Lee, Jongin Lim, Junghwan Song_  

... 175

Related-Key Attacks on DDP Based Ciphers: CIKS-128 and CIKS-128H

_Youngdai Ko, Changhoon Lee, Seokhie Hong, Jaechul Sung, Sangjin Lee_  

... 191

Cryptanalysis of Ake98

_Jorge Nakahara Júnior, Daniel Santana de Freitas_  

... 206

### Public Key Encryption

Designing an Efficient and Secure Public-Key Cryptosystem Based on Reducible Rank Codes

_Thierry Berger, Pierre Loidreau_  

... 218
**HEAD: Hybrid Encryption with Delegated Decryption Capability**  
*Palash Sarkar* .................................................. 230

**A Provably Secure Elliptic Curve Scheme with Fast Encryption**  
*David Galindo, Sebastià Martín, Tsuyoshi Takagi, Jorge L. Villar* ................................................... 245

**Efficient Representations**

*Advances in Alternative Non-adjacent Form Representations*  
*Gildas Avoine, Jean Monnerat, Thomas Peyrin* ................. 260

**Public Key Cryptanalysis**

*Attacks on Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups*  
*Françoise Levy-dit-Vehel, Ludovic Perret* ......................... 275

*Exact Analysis of Montgomery Multiplication*  
*Hisayoshi Sato, Daniel Schepers, Tsuyoshi Takagi* .............. 290

*Cryptography, Connections, Cocycles and Crystals: A p-Adic Exploration of the Discrete Logarithm Problem*  
*H. Gopalkrishna Gadiyar, KM Sangeeta Maini, R. Padma* .......... 305

**Modes of Operation**

*EME*: Extending EME to Handle Arbitrary-Length Messages with Associated Data  
*Shai Halevi* .......................................................... 315

*Impossibility of Construction of OWHF and UOWHF from PGV Model Based on Block Cipher Secure Against ACPCA*  
*Donghoon Chang, Wonil Lee, Seokhie Hong, Jaechul Sung, Sangjin Lee, Soohak Sung* .......................... 328

*The Security and Performance of the Galois/Counter Mode (GCM) of Operation*  
*David A. McGrew, John Viega* ........................................ 343
Signatures

Revisiting Fully Distributed Proxy Signature Schemes
  Javier Herranz, Germán Sáez ........................................ 356

New ID-Based Threshold Signature Scheme from Bilinear Pairings
  Xiaofeng Chen, Fangguo Zhang, Divyan M. Konidala,
  Kwangjo Kim .......................................................... 371

Separable Linkable Threshold Ring Signatures
  Patrick P. Tsang, Victor K. Wei, Tony K. Chan, Man Ho Au,
  Joseph K. Liu, Duncan S. Wong .................................... 384

Traitor Tracing and Visual Cryptography

A New Black and White Visual Cryptographic Scheme for General
Access Structures
  Avishek Adhikari, Tridib Kumar Dutta, Bimal Roy ............... 399

Identification Algorithms for Sequential Traitor Tracing
  Marcel Fernandez, Miguel Soriano ............................... 414

Author Index .......................................................... 431
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 approaches. 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.
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 $B$.

1.2 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 preva-
ence of communications on public (including wireless) networks it is more widely
recognised as an issue. For example, the Internet Key Exchange (IKE) proto-
col [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 mini-
aturisation 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 inter-
est 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 pro-
viding 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
added a set of “robustness principles” aimed specifically at protocols in the public-key setting.

The Abadi-Needham principles can be viewed as common sense rules that can be applied in an informal protocol design process. Undoubtedly the informal design of simple protocols has benefited from wide knowledge of these rules. However, it is interesting to note that at least two, and arguably four, of the rules are about clearly defining various aspects of the protocol specification. In addition two of the seven principles of Anderson-Needham fall into this category. In other words these informal rules can be regarded as promoting the use of formality in protocol analysis.

One of the principles of Abadi and Needham can be roughly paraphrased as ‘sign-before-encrypting’. In other words, when it is required to provide both authentication and confidentiality to some data, the plaintext should be signed and the result should then be encrypted. The idea behind this rule is intuitively clear: a signature of a ciphertext does not imply that the signer ever knew the plaintext. Indeed, there are several protocol attacks in which a signature on a ciphertext is removed by the adversary and replaced with a new signature. It is therefore somewhat surprising to find that many successful protocols, even those with proofs of security, ignore this rule. Paradoxically, much later analysis of the security of combining authenticity and encryption [ADR02] indicates that signing before encryption tends to give security properties no stronger than applying these operations the other way around.

3 Formal Specifications

Formal methods of specification and analysis, usually supported by software tools, have been used to analyse key establishment protocols for over 15 years. The typical analysis model uses a paradigm introduced by Dolev and Yao [DY83] in which cryptography is treated as a ‘black-box’ operation. This means that the adversary is able to encrypt and decrypt with any keys that it knows, but without the necessary keys will be unable to do anything with a ciphertext. Numerous formalisms and tools have been used over the years. Generally the tools search the available state space and try to establish whether insecure states can be reached. Various methods have been used to enhance the searching process. Meadows [Mea03] provides a detailed introduction to the history and progress of this research area.

3.1 Successes

There are some well-documented cases of new and unexpected attacks on protocols that have been found by machine analysis. The most celebrated is Lowe’s discovery [Low96] of a flaw in the public-key protocol of Needham and Schroeder [NS78] which was found in 1996, close to 20 years after the protocol’s first publication. The attack is surprisingly simple and once seen looks very obvious and not at all something beyond the capacity of a systematic search by hand.
In addition to finding flaws many protocols have been certified as free from flaws using analysis of formal specifications. Model checkers can be used to check protocols quickly and in an automated fashion. As one recent example, Basin et al. [BMV03] report that their ‘on-the-fly model checker’ (OFMC) was able to check all 36 protocols from the well known Clark–Jacob library [CJ97] in less than one minute of processing time.

### 3.2 Failures

A major limitation of models based on Dolev-Yao is that there is no succinct representation of the security property attained by a protocol that passes the analysis. What we know is that there is no adversary that can gain the stated secrets using the operations in the way specified. But that does not mean that there are not other strategies for the adversary that may be successful. Backes and Schunter [BS04] describe an example in which a mobile agent security protocol was formally verified to be secure with an automated theorem prover and yet it turned out to be vulnerable to a simple attack. Backes and Schunter point out that the reason for this failure was the omission of a critical action which the adversary should be allowed. Once the attack is discovered it is easy to include this action into the adversary’s repertoire. A possible conclusion is that you need to already know about the potential types of attack in order to find them using the this type of model. It is perhaps harsh to regard this example as a criticism of formal methods, since protocols of the type used in this case have not yet been modelled at all using the computational models described below.

A second, and more obvious, limitation of the Dolev-Yao approach is that the cryptographic properties are not modelled faithfully. One aspect of this is that partial information leakage and probabilistic behaviour is typically ignored. A related, practically significant, issue is that different definitions of confidentiality are not distinguished. In the cryptographic community there are several different standard definitions of confidentiality including indistinguishability and non-malleability, and protection against either known plaintext or chosen plaintext attacks. Generally algorithms with stronger properties are less efficient and require stronger assumptions, so it is a good principle to use the weakest assumptions possible regarding the cryptographic algorithm required. Having found the attack on Needham-Schroeder protocol mentioned in Section 3.1, Lowe proposed an improvement which showed no weaknesses using his technique. However, neither in the original definition, nor in his improved protocol, is there a specification of the encryption algorithm to be used in terms of the standard definitions. It is not hard to see that some form of non-malleability must be provided and Lowe does point out that the adversary must not be able to alter an encrypted message. Recently Warinschi [War03] has given a computational proof assuming that the encryption algorithm has a strong security property.

### 3.3 Prospects

There is no doubt that research using formal methods for protocol analysis is as active as it ever has been. The plethora of tools and formalisms that were ap-
plied during the 1990s revealed new insights but it is now widely recognised that advances are required to ‘go beyond Dolev-Yao’ by incorporating new properties and exploring new requirements. Meadows [Mea03] provides a comprehensive review of future trends. Some of the main directions that she mentions are coverage of denial of service, anonymity, and more cryptographic properties. Meadows remarks on the trend to analyse real-world protocols, particularly those in standards. Backes and Schunter [BS04] provide a “cryptographers’ wish-list” of Dolev-Yao extensions which overlaps with the issues identified by Meadows.

None of the current tools can really be used as design methods except in the sense that there are some (relatively) automatic and quick analysis tools that can be used to provide quick feedback on prototype designs. Meadows [Mea03] remarks that a possible direction towards using animation to help designers does not seem to be developing. There has been some work using tools to search for good protocols in the set of all possible protocols [CJ02]. So far it is not demonstrated that these can find useful new protocols with specified properties.

4 Provable Security

The cryptographic research community has evolved in the past 10-15 years to embrace formal foundations based on computational definitions and reductionist proofs. Acceptance of the approach is now widespread although there remain controversies [KM04], particularly when the so-called random oracle model is adopted. Initially the computational definitions concentrated on basic algorithms such as encryption and signature schemes. Key establishment was first considered in 1993 and interest has blossomed since the late 1990s.

4.1 Bellare–Rogaway Model

Bellare and Rogaway [BR93] initiated the computational study of key establishment in 1993. Their first paper covered only a two-party protocol between two users who already share a long-term key. Two years later [BR95] this was extended to a three-party protocol including a trusted server in the style of Needham and Schroeder’s shared key protocol.

In models of this type the adversary runs the protocol in the sense that it controls which parties send and receive messages. To do this the adversary issues a Send query. The adversary has the ability to fabricate any messages that it can compute and use these as messages. In addition the adversary can obtain any session key that has been accepted by issuing a Reveal query regarding any party instance. The adversary can also issue a Corrupt query regarding any party and obtain and modify its long terms keys. These capabilities model the ability of a protocol adversary to mount replay attacks and insider attacks. The adversary eventually issues a Test query for a session that has not been opened by a Reveal or Corrupt query. The adversary’s goal is to reliably distinguish between the key accepted in the test session and a random key. This is a strong definition of security but one which corresponds to the prevailing definition of security for confidentiality in encryption algorithms. The adversary is restricted only in
that it has bounded computational power; specifically it must be a probabilistic polynomial time algorithm.

**Successes.** By now there have been quite a few protocols proven secure in the Bellare–Rogaway model, or close variants. These include public key transport protocols, key agreement protocols, password-based protocols, multi-party key agreement and identity-based protocols. One may argue that the number of proven secure protocols is nevertheless quite small in comparison with the range of key establishment protocols currently known. Proving a protocol in this model is no small undertaking and most of the relevant papers contain proofs for only one or two protocols and require several pages of human-generated mathematical reasoning.

**Failures.** One criticism of the provable security approach in general is inaccessibility of the proofs. This leads in turn to a lack of wide scrutiny of the proofs [KM04]. There have been well-publicised failures in computational proofs for encryption. Proofs have also been claimed for key establishment protocols that were subsequently shown to be insecure. A protocol designed for low-power devices by Jakobsson and Pointcheval was initially published in a pre-proceedings version which was shown by Wong and Chan to be vulnerable to a simple masquerading attack [WC01]. Subsequently the protocol was fixed with a small change.

Another issue is whether protocols proven secure can be implemented in a way that they can be practically used. An important part of the security definition requires the identification of the partner of any principal in a protocol run. This is because the adversary must be forbidden from obtaining a session key in a trivial way by revealing the key from a partner who has accepted. In different versions of the Bellare–Rogaway model partnering has been defined in different ways. The most recent versions [BPR00] used the natural idea of session identifiers. This way of defining partners is not only intuitively clear (thus making the proofs more transparent) but also gives a practical way for entities to identify which key to use (for example on a particular communications socket). It turns out that the 1995 protocol proven secure by Bellare and Rogaway [BR95] has no reasonable way to define session identifiers. This means that although the protocol is secure it does not seem very useful. Choo *et al.* [CBHM04b] showed how a simple change to the protocol allows a natural session identifier to be defined, which can also be used in the protocol proof.

**Prospects.** Over the ten years and more since Bellare and Rogaway introduced their model there have been significant extensions. This has usually taken the form of new capabilities made available to the adversary to fit new requirements. For example, password-based protocols are accommodated by restricting the adversary’s ability to use *Send* queries since each such query may be used to test a single password. Instead a new *Execute* query allows the adversary to observe protocol runs without trying a password guess.
Although the basic model is now firmly established, it seems likely that new variations will continue to evolve to cater for new requirements. Very recently Abdalla et al. [AFP04] proposed a variation in the adversary capability which allows multiple Test queries which consistently respond with the real key or a random one. Looking back at some of the additional requirements mentioned in Section 1.2 we can see that there is potential for some new additions to the model. Forward secrecy is already catered for through use of the Corrupt query, but key compromise impersonation and anonymity do not yet seem to have been modelled. These two seem to be quite achievable in this type of model, but denial of service is an area that seems to fall outside the scope of the usual computational models.

It is clear that analysis in the Bellare–Rogaway model does not provide an efficient way to design a new protocol. Varying an existing protocol is very likely to break an existing proof and there seems no useful way to guess whether a proof is possible for a new protocol.

4.2 Modular Proofs

In 1998, Bellare, Canetti and Krawczyk [BCK98] suggested a method for modular proofs of key establishment protocols. The basic idea is to first prove the protocol secure in an ideal world where messages are automatically authenticated. This ideal world is called the authenticated links model or simply the AM. This roughly corresponds to the situation where the adversary is passive, so unable to alter or fabricate messages (although the adversary is able to effectively delete messages). Having proved the protocol secure in the ideal world it can then be transformed into a protocol in a more realistic model in which the adversary does have the ability to fabricate messages — indeed the capabilities of the adversary are basically the same as those in the Bellare–Rogaway model.

The initial model of Bellare et al. [BCK98] used a security definition based on emulation between protocols in the two worlds. Later it was found that this definition is too strict to be useful and so, in 2001, Canetti and Krawczyk published a revised model [CK01] with a definition of security based on indistinguishability, similar to that of Bellare and Rogaway. Another significant benefit in the new model is that it is proven that the agreed session key can be used safely to provide secure channels, a property absent from the Bellare–Rogaway model.

Successes. The modular approach uses two types of components: the simplified protocols in the ideal world (called AM protocols) and the compilers to transform protocols into the real world (called authenticators). One of the significant benefits of the modular approach is the ability to reuse any AM protocol with any authenticator. Consequently, when one new component is proven secure, a whole set of new protocols results whose members are all automatically proven secure. As the number of components increases the multiplying effect of adding other components becomes more significant.

The separation of concerns between session key confidentiality and authentication also allows a much easier way to select components suitable for different applications. In other words, we may regard the modular approach as a step