Carlo Blundo
Stelvio Cimato (Eds.)

LNCS 3352

Security in Communication Networks

4th International Conference, SCN 2004
Amalfi, Italy, September 2004
Revised Selected Papers

Springer

Carlo Blundo Stelvio Cimato (Eds.)

Security in Communication Networks

4th International Conference, SCN 2004
Amalfi, Italy, September 8-10, 2004
Revised Selected Papers

Springer

Volume Editors

Carlo Blundo
Stelvio Cimato
Università degli Studi di Salerno, Dipartimento di Informatica ed Applicazioni
84081 Baronissi (SA), Italy
E-mail: {carblu, cimato}@dia.unisa.it

Library of Congress Control Number: 2004117660

CR Subject Classification (1998): E.3, C.2, D.4.6, K.4.1, K.4.4, K.6.5, F.2

ISSN 0302-9743
ISBN 3-540-24301-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11375937 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3352

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Preface

The 4th International Conference on Security in Communication Networks 2004 (SCN 2004) was held at the "Diocese Hall" of the Archdiocese of Amalfi-Cava de' Tirreni and the "Armorial Bearings Hall" of the Archbishop Palace in Amalfi, Italy, on September 8–10, 2004. Previous conferences also took place in Amalfi in 1996, 1999 and 2002.

The conference aimed at bringing together researchers in the fields of cryptography and security in communication networks to foster cooperation and the exchange of ideas.

The main topics included all technical aspects of data security, including: anonymity, authentication, block ciphers, complexity-based cryptography, cryptanalysis, digital signatures, distributed cryptography, hash functions, identification, implementations, key distribution, privacy, public key encryption, threshold cryptography, and zero knowledge.

The Program Committee, consisting of 21 members, considered 79 papers and selected 26 for presentation; one of them was withdrawn by the authors. These papers were selected on the basis of originality, quality and relevance to cryptography and security in communication networks.

Due to the high number of submissions, paper selection was a difficult and challenging task, and many good submissions had to be rejected. Each submission was refereed by at least three reviewers and some had four reports or more. We are very grateful to all the program committee members, who devoted much effort and valuable time to read and select the papers. In addition, we gratefully acknowledge the help of colleagues who reviewed submissions in their areas of expertise. They are all listed on page VII and we apologize for any inadvertent omissions.

These proceedings include the revised versions of the 26 accepted papers and the abstract of the invited talk by Bart Preneel (*ECRYPT: the Cryptographic Research Challenges for the Next Decade*).

Following the example of the previous editions of SCN, we encouraged authors to submit their contributions in electronic format. We handled the submissions with CyberChair (http://www.CyberChair.org) a free Web-based paper submission and reviewing system.

Finally, we would like to thank all the authors who submitted their papers for making this conference possible, the Program Committee members, as well as all the conference participants.

September 2004

C. Blundo
S. Cimato

SCN 2004

September 8–10 2004, Amalfi, Italy

Program Chair

Carlo Blundo	Università di Salerno, Italy

General Chair

Stelvio Cimato	Università di Salerno, Italy

Program Committee

Giuseppe Ateniese	Johns Hopkins University, USA
Carlo Blundo	Università di Salerno, Italy (Chair)
Christian Cachin	IBM Research, Switzerland
Ran Canetti	IBM Research, USA
Xiaotie Deng	City University, Hong Kong, China
Alfredo De Santis	Università di Salerno, Italy
Yvo Desmedt	University College London, UK
Giovanni Di Crescenzo	Telcordia Technology, USA
Rosario Gennaro	IBM Research, USA
Eyal Kushilevitz	Technion, Israel
Tanja Lange	University of Bochum, Germany
Ueli Maurer	ETH Zurich, Switzerland
Eiji Okamoto	Tsukuba University, Japan
Rafail Ostrovsky	UCLA, USA
Giuseppe Persiano	Università di Salerno, Italy
Leonid Reyzin	Boston University, USA
Rei Safavi-Naini	University of Wollongong, Australia
Jacques Stern	ENS, France
Doug Stinson	University of Waterloo, Canada
Gene Tsudik	UCI, USA
Moti Yung	Columbia University, USA

Local Organizing Committee

Paolo D'Arco	Università di Salerno, Italy
Barbara Masucci	Università di Salerno, Italy

Sponsoring Institutions

Dipartimento di Informatica ed Applicazioni, Università di Salerno, Italy
Lanfredi Fund, France

Referees

Michel Abdalla
Joonsang Baek
Amos Beimel
Jan Camenisch
Claude Castelluccia
Dario Catalano
Xi Chen
Qi Cheng
Hung Chim
Stelvio Cimato
Paolo D'Arco
Breno de Medeiros
Xuhua Ding
Pierre-Alain Fouque
Clemente Galdi
Louis Granboulan
Matthew Green
Daniel Hamburg
Jason Hinek
Seny Kamara
Aggelos Kiayias
Hugo Krawczyk
TieYan Li
Becky Liu
John Malone-Lee
Barbara Masucci
Lan Nguyen
Phong Nguyen
David Pointcheval
David Safford
Willy Susilo
Nicolas Tadeusz Courtois
Ivan Visconti
Duncan Wong
Shouhuai Xu
Jianhong Zhang
Huafei Zhu

Table of Contents

Invited Talk

Reduction of Security/Primitives

Signature Schemes

Anonymity and Privacy

Authentication and Identification

Zero Knowledge

Public Key Cryptosystems

Distributed Cryptography

Cryptanalysis of Public Key Cryptosystems

Cryptanalysis

Email Security

Key Distribution and Feedback Shift Registers

ECRYPT: The Cryptographic Research Challenges for the Next Decade

B. Preneel

Katholieke Univ. Leuven, Dept. Electrical Engineering-ESAT,
Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
bart.preneel@esat.kuleuven.ac.be

Abstract. In the past thirty years, cryptology has evolved from a secret art to a modern science. Weaker algorithms and algorithms with short keys are disappearing, political controls of cryptography have been reduced, and secure cryptography is becoming more and more a commodity. Moreover, implementations are being becoming more secure as well. This progress may lead to the belief that the cryptography problem is "solved." However, this article discusses some of the challenging problems ahead in the area of cryptographic algorithms and protocols. We also explain how the ECRYPT Network of Excellence (www.ecrypt.eu.org) tries to address some of the challenges by bringing together 250 European researchers in the area of cryptology and the related area of watermarking.

1 Introduction

While cryptology is getting increasingly important in the information society, it is also becoming less and less visible. Cryptology has been integrated into smart cards for financial transactions, web browsers, operating systems, mobile phones and electronic identity cards. This success can be explained by several factors: first, there is a clear need for cryptographic solutions, second adequate algorithms and protocols have been developed, and third the decreasing cost of computation makes it inexpensive to implement symmetric and even asymmetric cryptology. For outsiders, who have limited understanding of the complexity of the field, the widespread deployment of cryptology may give the impression that there a no important problems left in cryptography. We have cryptographic algorithms and protocols available that can be called as a "black box" by security engineers to solve some standard problems and the security and performance of these implementations is improving.

Consequently, one may believe that research efforts in security should be focused exclusively on building trust infrastructures and integrating security into applications. This (incorrect) impression is strengthened by the (correct) observation that security systems fail usually due to other reasons than cryptographic flaws (such as incorrect specifications or implementations, bad management, viruses, social engineering attacks...) [2].

C. Blundo and S. Cimato (Eds.): SCN 2004, LNCS 3352, pp. 1–15, 2005.

A second (but incorrect) conclusion that one may draw from these observations is that research discipline cryptology has ran out of practical problem, and hence researchers now work on purely theoretical problems such as general multi-party computation, exotic protocols and on the question whether or not one-way functions exist. Any cryptographic protocol (encryption, authentication, key establishment, e-payment, e-voting, ...) can be described as a multi-party computation, and generic but highly inefficient solutions to this problem are known since the late 1980s [5, 12, 25]. An interesting challenge is to make these protocols more efficient, either in the general case or for concrete problems (such as group signatures or e-voting) for example by introducing stronger cryptographic assumptions. The most fundamental assumption is the existence of one-way functions: while our intuition seems to suggest that it is very easy to design a function that is "easy" to compute but "hard" to invert, so far the best theoretical result can prove that there exist functions that are twice as hard to invert as to compute [27]; it is clear that such functions would be completely useless to practical cryptology. This is quite remarkable, since one-way functions are a cornerstone of cryptology.

Section 2 presents an overview of the challenges that remain in both practical and theoretical cryptography. Since the area of cryptology is rather broad, the emphasis will be on symmetric cryptology by summarizing the status after recent attacks on block ciphers, stream ciphers and hash functions. We briefly address some research issues in asymmetric cryptology, but due to lack of space we do not provide details on areas such as protocols, secure implementation, watermarking, and perceptual hashing. Next we attempt to explain the problems problems that arise in the standardization of cryptographic algorithms and protocols. Section 3 explains how the ECRYPT project intends to address some of these research challenges. Some concluding remarks are presented in Sect. 4.

2 Research Challenges in Cryptology

2.1 State of the Art

Most of the applications are covered by the block ciphers triple-DES [19] and AES [20]; DES, which was widely used until the late 1990s, is being replaced quickly (NIST has announced in July 2004 that it will withdraw support for the DES algorithm since its strength is no longer sufficient to adequately protect Federal government information). In addition 3rd generation mobile networks (3GPP) use KASUMI [1] and Bluetooth uses SAFER+ [8]. While military environments still use proprietary stream ciphers, RC4 [24] is widely deployed in the commercial world (e.g., SSL/TLS, WEP); GSM uses the stream ciphers A5/1 and A5/2 [7, 42] and Bluetooth uses E0 [8]. The most popular hash functions are MD5 [37], which was broken in August 2004 [43], SHA-1 [23] and in some applications RIPEMD-160 [17] and MDC-2 (see [35]). For MAC algorithms, HMAC and several variants of CBC-MAC are widely used. In the area of public-key cryptology, RSA [38] is clearly the most popular algorithm, both for public key encryption and for digital signatures. For digital signatures, DSA, ECDSA (Elliptic Curve DSA) and variants of these are also successful. For public key encryption, ElGamal and some elliptic curve variants can also be found in applications. For key establishment several variants of authenticated Diffie-Hellman are widely deployed. For entity authentication, there is a limited use of zero-knowledge protocols, o.a. in the pay-TV world and in Novell networks. It is not feasible within the scope of this article to discuss in detail all the cryptographic algorithms and protocols included in standards such as SSL/TLS, IPsec/IKE, SSH, S/MIME, PGP, GSM, 3GPP, WEP, WPA, RSN, Bluetooth, EMV, Global Platform, ... It is clear that this could be a useful exercise to assess the impact of developments in cryptology.

2.2 Challenges

In this section we discuss the research challenges from a generic perspective. Even if we have currently a large toolbox of cryptographic algorithms and protocols, this may not be adequate for the next years due to several reasons. A first issue is the changing environment and threat models in which cryptology will be deployed: we are evolving towards ambient intelligence, pervasive networking or ubiquitous computing, which have completely new characteristics. A second element is the gradual erosion of the computational difficulty of the mathematical problems on which cryptology is based; this erosion is created in part by developments in computation (progress in electronics and in the future in optical and maybe even quantum computing) and in part by progress in cryptanalytic algorithms. A final element is the requirements of new applications and cryptographic implementations, including the lack of physical security in devices.

In order to structure these new requirements, the areas in which further research is needed can be organized according to three parameters: cost (hardware, memory, power), performance (throughput, latency) and security level. Ideally one would like to achieve a high security level and a high performance at a low cost, but this is not feasible. In practice one has to focus on at least one criterion; depending on the choice, one obtains different solutions. Within this choice, there may still exist trade-offs between the remaining two parameters.

Low Cost and/or Low Power: this can be achieved by giving up high performance or high security; this approach is essential to allow for integration of cryptography in even the tiniest devices (e.g., ambient intelligence). Design goals could be the implementation of a stream cipher that offers a reasonable security level (say 80 bits) with uses less than 1000 gates.

High Performance: this is required for highly efficient solutions for applications such as bus encryption, hard disk encryption, encryption in Terabit networks. If cryptography presents too large an overhead/cost, it will not be deployed, or it will be switched off. In this context, it is important to note that while Moore's 'law' predicts that in 2018, the computational power for the same cost will have increased with a factor of about 100, Gilder's 'law' predicts that the speed of LANs and storage devices will increase with a factor of 10 000. This shows that parallelism will become increasingly important in cryptographic operations, but also demonstrates the need for high performance designs.

High Security: some application areas require cryptographic algorithms and protocols that can offer a higher confidence and assurance level than the state of the art. E.g., for e-voting, we need secure and robust protocols that survive even if a subset of the players are faulty or corrupt and that provide long-term security; for e-health and national security we need cryptographic algorithms which provide guaranteed protection for 50 years or more. As an example, information on our DNA has implications on the DNA of our children and grandchildren, hence this is information that may need to be protected for a very long time.

These requirements guide the approaches taken by the research teams in the ECRYPT project (cf. Sect. 3).

2.3 Symmetric Cryptology

In this section we comment on the challenges in the area of block ciphers, stream ciphers and cryptographic hash functions; we omit MAC algorithms for two reasons: they are mostly derived from other block ciphers and hash functions, and highly efficient constructions based on universal hash functions are known (even if they are not yet widely used).

Block Ciphers. The area of block ciphers has always been very particular in cryptology due to the availability of widely supported standards. The impact of the publication of the Data Encryption Standard (DES) in 1977 by the US NIST [33] (at that time called NBS) on both practice and research is hard to overestimate. DES was obtained after an open competition, in which IBM provided the winning entry; the final design was performed by IBM in cooperation with NSA. After some initial controversy, DES became widely used, first in the financial sector and later on in a broad range of applications.

In the 1990s it became clear that the key length of DES (56 bits) was no longer adequate (see for example Wiener [44]); moreover, the block length of 64 bits will also be too short in the next decade, which means that triple-DES (which is also rather slow) is not an adequate replacement. Therefore NIST launched a call for a successor in 1997. After an open competition with 22 entries, NIST selected the Belgian Rijndael algorithm (designed by J. Daemen and V. Rijmen) as the winner in October 2000. The AES standard FIPS 197 (Federal Information Processing Standard) was published in December 2001 [20]; it is a 128-bit block cipher with a key of 128, 192 and 256 bits. AES is mandatory for sensitive but unclassified data. In 2003, the US government announced that AES can also be used for classified information up to the secret level, while AES with key lengths of 192 and 256 bits can be used for top secret information. In software, AES is more than twice as fast as DES, and thus significantly faster than triple-DES.

In 2004, AES has been included in more than thousand products, and as of August 2004, 171 AES product certifications have been performed by NIST. AES is being adopted very quickly as a standard in other environments (IETF, ISO, IEEE, 3GPP, ...), with the exception of the financial sector, which is finalizing its slow migration from DES to triple-DES.

While there was a broad consensus on the choice by NIST, there were also some critical comments on the algebraic structure present in the AES. This structure allows for an elegant description and efficient implementations both in hardware and software (8-bit and 32-bit machines), but may also induce weaknesses. For example, it was shown by Courtois and Pieprzyk [11] that the algebraic structure in the AES S-box leads to simple quadratic equations. The authors of [11] claim that it may be possible to solve these equations faster than an exhaustive key search. See also more recent work on algorithms [3, 13] to solve quadratic equations. Murphy and Robshaw have shown that the simple overall structure leads to an embedding in larger block cipher BES [31], which has certain weaknesses; however, these weaknesses do not seem to apply to AES. Finally, several authors have shown that the algebraic structure leads to equivalent descriptions of the AES.

In conclusion, more than two years after the announcement of these properties, none of these attacks seems to pose a realistic threat to the security of AES. It is clear that in view of the importance of the AES, more research is needed to increase our understanding of this algorithm. On the other hand, in the past 15 years the cryptographic community has built up some extensive design expertise for block ciphers; even if it would turn out that a less elegant (and less mathematical) design is more desirable, it would not be too difficult to modify the design accordingly.

Stream Ciphers. In contrast to block ciphers, the area of stream cipher has been characterized by many proprietary algorithms and a lack of standards. The first generation of stream ciphers (1920s–1950s) used mechanical and electromechanical designs based on rotors. Subsequently, electronic designs were developed using Linear Feedback Shift Registers (LFSRs); an extensive mathematical theory has been created to analyze these stream ciphers. In the last 15 years a new generation of software-oriented stream ciphers has been proposed, which uses word lengths between 8 and 32 bits and runs efficiently on modern processors.

Designing a secure stream cipher should in principle be easier than designing a block cipher, since a stream cipher has an internal state that cannot be influenced by the opponent (there is no equivalent of a chosen plaintext attack). However, stream cipher designers aim for a significantly better performance than a block cipher in OFB (Output FeedBack) or CTR (CounTeR) mode, which is a natural benchmark. As a consequence, output bits are produced after a few operations, which implies that mixing may be less thorough as desirable. In addition, new attack models are being introduced which exploit the fact that the output stream needs to be restarted or re-synchronized at regular intervals using an Initialization Vector (IV). A chosen IV attack gives an opponent some control over the initialization of the internal state.

The rich algebraic algebraic structure of LFSRs has resulted in a large number of attack strategies: linear attacks, algebraic attacks, correlation attacks, divide and conquer attacks, ... As a consequence, some researchers are convinced that LFSRs should be eliminated altogether from the design of a stream cipher. As an alternative, one could consider the T-functions proposed by Klimov and Shamir [29]; these functions provide an efficient implementation of a single-cycle non-linear iteration on 2^n bits.

Software-oriented stream ciphers have been analyzed using an ad-hoc approach, that use a broad variety of techniques. The NESSIE project [32], which organized an open competition to develop standard proposals for cryptographic algorithms, concluded that none of the submitted stream ciphers satisfied the security criteria. In most cases, the attacks found were so-called distinguishing attacks with a very high data complexity, which may not represent a realistic threat on applications. However, the NESSIE project asked for a very high security margin, and the submitters initially believed that they could provide this. The motivation was to obtain a sufficient security margin for long-term security. More research is needed to evaluate to which extent we need to reduce the security requirements to obtain the expected performance benefit from stream ciphers.

In order for stream ciphers to be useful in practice, they may also need efficient resynchronization procedures, and an optional mode for authenticated encryption. There is clearly a need for standardized stream ciphers that offer either a very low cost (in terms of gate count or power) or that are highly efficient in software. ECRYPT intends to this

Hash Functions. The area of hash functions has been characterized by a large number of broken schemes in their 25-year history (see [34, 35] for an overview). In practice however, only a limited number of schemes are widely used: MD5 and SHA-1, and to a limited extent RIPEMD-160 and MDC-2.

MD4 was proposed by Rivest in 1990 and broken by Dobbertin in 1996 [16]. MD5 was proposed one year later as a strengthened version of MD4. However, it was discredited by attacks by den Boer and Bosselaers in 1992 [15] and Dobbertin in 1996 [18]; the last attack led RSA Security to withdraw its support for new applications. These attacks showed serious weaknesses of the compression function of MD5, but they did not provide collisions for the complete function. In the mean time, brute force collision attacks on MD5 – which require 2^{64} operations only – are also within reach. In spite of these development, MD5 remained widely used in a broad range of applications until today. In August 2004, four researchers (X. Wang, D. Feng, X. Lai, and H. Yu) announced that they had found collisions for MD5 [43]; their attack requires only 15 minutes on a normal laptop.

The Secure Hash Algorithm, was proposed by NIST [21] in 1993; SHA has a 160-bit hash result. After one year, NIST discovered a certificational weakness in SHA; apparently collisions could be found in less than 2^{80} operations. Consequently a new release of the standard was published. The new algorithm is called SHA-1 [22], which prompted some researchers to rename the original SHA as SHA-0 (this has created some confusion).

After work by Chabaud and Joux in 1998 [10], Biham and Chen in 2004 [6], Joux, Carribault, Jalby and Lemuet presented a collision for SHA in August

2004 [28]; their attack requires 2^{51} compression function computations. Wang et al. [43] claim an improved attack that requires only 2^{40} compression function computations; however, this attack has not yet been implemented.

Biham and Chen have also investigated the extension of their attacks to SHA-1 [6]. The current status is that they can find collisions for 43 (out of 80) rounds of SHA-1; they also show that finding collisions for up to 53 (out of 80) rounds of SHA-1 is faster than a brute force collision attack, which requires 2^{80} steps of the compression function.

The implications of the new cryptanalytic techniques discovered in 2004 on SHA-1 and on RIPEMD-160 are still under study. At this time it is too early to make a reliable assessment, but there does not seem to be an immediate threat to either hash function; however, brute force attacks on these hash functions – requiring 2^{80} compression function evaluations – may become within reach within 10-15 years.

In 2004, Hawkes and Rose [26] have presented some critical observations on the security of SHA-256 (with a 256-bit result). While it is probably too early to draw firm conclusions, it seems now plausible that finding collisions for SHA-256 could take less than 2^{128} evaluations of the compression function, but it may still be out of reach for the next 20 years or more.

For the time being, there is still a lack of understanding of the security of hash function designs. Most practical constructions build on the original ideas of MD4 (32-bit arithmetic and logical operations); we have learned in the last decade that these designs are probably less secure than anticipated. The next generation standards SHA-256 through SHA-512 [23] offers better security levels based on similar principles. However, they are also significantly slower than SHA-1 (about 2-6 times) and it may be that some of the new attack techniques can be extended to these designs.

2.4 Asymmetric Cryptology

The research challenges in asymmetric cryptology are certainly not smaller. The first results in security reductions focused on asymmetric cryptology; in this line of research, one attempts to prove that the security of a cryptographic primitive or protocol can be reduced to an assumption on the difficulty of a mathematical problem (such as extracting modular roots, factoring the product of two large primes or solving the discrete logarithm problem in a specific group). Research concentrates on finding efficient and meaningful reductions, on reducing assumptions used in the proof (such as the 'random oracle model' [4, 9]), on establishing relations between assumptions, and on finding primitives with better and/or more complex security properties. It should also be pointed out that the security of most asymmetric primitives depends on a small set of problems from algebraic number theory; any breakthrough in solving some of these problems could have dramatic consequences. This shows that there is a need for new asymmetric algorithms that depend on new problems.

Cryptology also needs to take into account the ever increasing speed of electronic computers; typically this can be addressed by an adequate upgrade path