


Jennifer Seberry Yuliang Zheng (Eds.)

Advances in Cryptology— AUSCRYPT '92

Workshop on the Theory and Application
of Cryptographic Techniques
Gold Coast, Queensland, Australia
December 13-16, 1992
Proceedings

Cc01-718



Springer-Verlag

Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Series Editors

Gerhard Goos
 Universität Karlsruhe
 Postfach 69 80
 Vincenz-Priessnitz-Straße 1
 D-76131 Karlsruhe, Germany

Juris Hartmanis
 Cornell University
 Department of Computer Science
 4130 Upson Hall
 Ithaca, NY 14853, USA

Volume Editors

Jennifer Seberry
 Yuliang Zheng
 Department of Computer Science, University of Wollongong
 Northfields Avenue, Wollongong NSW 2522, Australia

CR Subject Classification (1991): E.3-4, D.4.6, G.2.1, C.2.0, K.6.5

ISBN 3-540-57220-1 Springer-Verlag Berlin Heidelberg New York
 ISBN 0-387-57220-1 Springer-Verlag New York Berlin Heidelberg

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1993
 Printed in Germany

Typesetting: Camera-ready by authors
 Printing and binding: Druckhaus Beltz, Hemsbach/Bergstr.
 45/3140-543210 - Printed on acid-free paper

Preface

The AUSCRYPT'92 conference held on the Gold Coast, Queensland, Australia, 13-16 December, 1992 is the second conference held in the Southern Hemisphere in cooperation with the International Association for Cryptologic Research. The conference was very enjoyable and ran very smoothly, largely due to the efforts of the General Chair, Professor Bill Caelli of the Queensland University of Technology and his colleagues Ed Dawson, Barry Arnison, Helen Bergen, Eleanor Crosby, Diane Donovan, Ian Graham, Helen Gustafson, and Lauren Nielson. There were 114 attendees from 18 countries and 5 continents.

This is the third conference held outside the EUROCRYPT series, held in European countries each northern spring, and the CRYPTO series held in Santa Barbara, California, USA each August. The other two were AUSCRYPT'90 held in Sydney, New South Wales, Australia in January 1990 and ASIACRYPT'91 held in Fujiyoshida, Japan in December 1992.

There were 77 submissions from 18 countries and 55 were accepted from 15 countries. Thirty were submitted from Asia and 15 accepted, 17 from Europe and 13 accepted, 12 from North America and 8 accepted and 18 from Australia of which 9 were accepted. In addition there were 7 presentations representing 5 countries at the rump sessions. After refereeing, 3 of them were selected to be published in these proceedings. All refereeing was carried out blind: no names were attached to papers. Programme Committee members' submissions were anonymous and went through exactly the same refereeing procedure as all other papers except that they were always sent to referees not in their own country. In addition the Committee chose four invited speakers: Yvo Desmedt from University of Wisconsin-Milwaukee, USA, Peter Landrock, the IACR President from Denmark, Valery Korzhik from Russia and John Snare, Australia's representative on the International Standards Committees. Please remember that these invited talks were not refereed and the authors bear full responsibility for their contents.

It is our pleasure to acknowledge the efforts of all those who contributed to making the conference a success. We especially wish to thank the members of the Programme Committee: Mike Burmester (RHNBC, University of London, UK), Yvo Desmedt (University of Wisconsin-Milwaukee, USA), Hideki Imai (University of Tokyo but formerly of Yokohama National University, Japan), Svein Knapskog (University of Trondheim, Norway), Rudi Lidl (University of Tasmania, Hobart, Australia), John Loxton (Macquarie University, Sydney, Australia), Tsutomu Matsumoto (Yokohama National University, Japan), Josef Pieprzyk (University of Wollongong, New South Wales, Australia), Reza Safavi-Naini, (University of Wollongong, New South Wales, Australia) and the Programme Chair Jennifer Seberry (University of Wollongong, New South Wales, Australia). Many of these referees will have used other persons to advise and evaluate and we sincerely thank those anonymous persons. Josef Pieprzyk ably organized the Rump Session.

We must thank my two valuable helpers Tor Jomar Nordhagen (Norway) and Marc Gysin (Switzerland) who helped so much with the electronic processing, entering into the computer all referees' comments that came by snail mail, then helped to email and print letters for the acceptances and rejections so we could get comments to authors as speedily as possible.

We wish to thank all the authors for sending their submissions (even ones that were unsuccessful), the speakers, and all the participants of this and other IACR conferences. We have established a tradition for high quality research and we hope this continues.

Wollongong, New South Wales, Australia
July 1993

Jennifer Seberry
Yuliang Zheng

General Chair

Bill Caelli (Queensland University of Technology, Australia)

Program Chair

Jennifer Seberry (University of Wollongong, Australia)

Program Committee

Mike Burmester	(RHBNC, University of London, UK)
Yvo Desmedt	(University of Wisconsin-Milwaukee, USA)
Hideki Imai	(University of Tokyo, Japan)
Svein Knapskog	(University of Trondheim, Norway)
Rudi Lidl	(University of Tasmania, Australia)
John Loxton	(Macquarie University, Australia)
Tsutomu Matsumoto	(Yokohama National University, Japan)
Josef Pieprzyk	(University of Wollongong, Australia)
Rei Safavi-Naini	(University of Wollongong, Australia)

In cooperation with

The International Association for Cryptologic Research (IACR)
and

The Centre for Computer Security Research, University of Wollongong
and

The Information Security Research Centre, Queensland University of
Technology

Table of Contents

Session 1: AUTHENTICATION AND SECRET SHARING I

Chair: Diane Donovan

Threshold cryptosystems (invited talk)	3
<i>Y. Desmedt (University of Wisconsin-Milwaukee, USA)</i>	
Authentication codes with perfect protection	15
<i>L. Tombak, R. Safavi-Naini (University of Wollongong, Australia)</i>	
Practical proven secure authentication with arbitration	27
<i>Y. Desmedt (University of Wisconsin-Milwaukee, USA),</i> <i>J. Seberry (University of Wollongong, Australia)</i>	

Session 2: AUTHENTICATION AND SECRET SHARING II

Chair: Josef Pieprzyk

Authentication codes under impersonation attack	35
<i>R. Safavi-Naini, L. Tombak (University of Wollongong, Australia)</i>	
Cumulative arrays and geometric secret sharing schemes	48
<i>W.-A. Jackson (RHBNC, University of London, UK),</i> <i>K.M. Martin (University of Adelaide, Australia)</i>	
Nonperfect secret sharing schemes	56
<i>W. Ogata, K. Kurosawa, S. Tsujii (Tokyo Institute of Technology, Japan)</i>	
A construction of practical secret sharing schemes using linear block codes ..	67
<i>M. Bertilsson, I. Ingemarsson (Linköping University, Sweden)</i>	

Session 3: SIGNATURES AND HASHING ALGORITHMS

Chair: Yvo Desmedt

HAVAL — a one-way hashing algorithm with variable length of output	83
<i>Y. Zheng, J. Pieprzyk, J. Seberry (University of Wollongong, Australia)</i>	
On the power of memory in the design of collision resistant hash functions	105
<i>B. Preneel, R. Govaerts, J. Vandewalle (Katholieke Universiteit Leuven, Belgium)</i>	
A practical digital multisignature scheme based on discrete logarithms	122
<i>T. Hardjono (ATR Communications Research Laboratories, Japan),</i> <i>Y. Zheng (University of Wollongong, Australia)</i>	
Group-oriented undeniable signature schemes without the assistance of a mutually trusted party	133
<i>L. Harn (University of Missouri-Kansas, USA),</i> <i>S. Yang (University of Science and Technology of China, PRC)</i>	

Session 4: THEORY OF S-BOXES

Chair: Tsutomu Matsumoto

Highly nonlinear 0-1 balanced Boolean functions satisfying strict avalanche criterion	145
<i>J. Seberry, X.-M. Zhang (University of Wollongong, Australia)</i>	
Linear nonequivalence versus nonlinearity	156
<i>C. Charnes, J. Pieprzyk (University of Wollongong, Australia)</i>	
Constructing large cryptographically strong S-boxes	165
<i>J. Detombe, S.E. Tavares (Queen's University at Kingston, Canada)</i>	

Session 5: CRYPTANALYSIS

Chair: Peter Landrock

Nonasymptotic estimates of information protection efficiency for the wire-tape channel concept (invited talk)	185
<i>V. Korzhnik, V. Yakovlev (Bronch-Bruevitch Technical Communications University, Russia)</i>	
Cryptanalysis of LOKI91	196
<i>L.R. Knudsen (Aarhus University, Denmark)</i>	
Cryptanalysis of summation generator	209
<i>E. Dawson (Queensland University of Technology, Australia)</i>	

Session 6: PROTOCOLS I

Chair: Rei Safavi-Naini

Secure addition sequence and its applications on the server-aided secret computation protocols	219
<i>C.-S. Lai, S.-M. Yen (National Cheng Kung University, Taiwan)</i>	
Subliminal channels for signature transfer and their application to signature distribution schemes	231
<i>K. Sakurai (Mitsubishi Electric Co., Japan), T. Hoh (Tokyo Institute of Technology, Japan)</i>	
A practical secret voting scheme for large scale elections	244
<i>A. Fujioka, T. Okamoto, K. Ohita (NTT Laboratories, Japan)</i>	
Privacy for multi-party protocols	252
<i>T. Satoh, K. Kurosawa, S. Tsujii (Tokyo Institute of Technology, Japan)</i>	

Session 7: PROTOCOLS II

Chair: Ed Dawson

New protocols for electronic money	263
<i>J.C. Pailles (SEPT, France)</i>	
Modelling and analyzing cryptographic protocols using Petri nets	275
<i>B.B. Nieh, S.E. Tavares (Queen's University at Kingston, Canada)</i>	
On verifiable implicit asking protocols for RSA computation	296
<i>T. Matsumoto (Yokohama National University, Japan),</i>	
<i>H. Imai (University of Tokyo, Japan),</i>	
<i>C.-S. Lai, S.-M. Yen (National Cheng Kung University, Taiwan)</i>	
Modified Maurer-Yacobi's scheme and its applications	308
<i>C.H. Lim, P.J. Lee (Pohang Institute of Science and Technology, Korea)</i>	

Session 8: SEQUENCES

Chair: Rudi Lidl

The vulnerability of geometric sequences based on fields of odd characteristic	327
<i>A. Klapper (University of Manitoba, Canada)</i>	
A fast cryptographic checksum algorithm based on stream ciphers	339
<i>X. Lai (Swiss Federal Institute of Technology, Switzerland),</i>	
<i>R.A. Rueppel, J. Woollven (R³ Security Engineering, Switzerland)</i>	
An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure	349
<i>M.J. Mihajevic (University of Belgrade, Yugoslavia)</i>	
Construction of m -ary de Bruijn sequences	357
<i>J.-H. Yang, Z.-D. Dai (Academia Sinica, PRC)</i>	

Session 9: PSEUDORANDOMNESS

Chair: Bill Caelli

Information technology security standards — an Australian perspective (invited talk)	367
<i>J. Snare (Telecom Research Laboratories, Australia)</i>	
Non-interactive generation of shared pseudorandom sequences	385
<i>M. Cerecedo, T. Matsumoto (Yokohama National University, Japan),</i>	
<i>H. Imai (University of Tokyo, Japan)</i>	
A generalized description of DES-based and Benes-based permutation generators	397
<i>M. Portz (RWTH Aachen, Germany)</i>	

Session 10: ODDS AND ENDS

Chair: Valery Korzhik

Prime generation with the Demytko-Miller-Trbovich algorithm	413
<i>L. Condie (University of New England, Australia)</i>	
Construction of feebly-one-way families of permutations	422
<i>A.P.L. Hiltgen (Swiss Federal Institute of Technology, Switzerland)</i>	
On bit correlations among preimages of	
“many to one” one-way functions	435
<i>K. Sakurai (Mitsubishi Electric Co., Japan),</i>	
<i>T. Itoh (Tokyo Institute of Technology, Japan)</i>	
The fast cascade exponentiation algorithm and	
its applications on cryptography	447
<i>S.-M. Yen, C.-S. Lai (National Cheng Kung University, Taiwan)</i>	

Session 11: PUBLIC KEY CRYPTOGRAPHY I

Chair: Jennifer Seberry

The design of a conference key distribution system	459
<i>C.-C. Chang (National Chung Cheng University, Taiwan),</i>	
<i>T.-C. Wu (National Chiao Tung University, Taiwan),</i>	
<i>C.-P. Chen (National Chung Cheng University, Taiwan)</i>	
Remarks on “The design of a conference key distribution system”	467
<i>E. Zuk (Telecom Research Laboratories, Australia)</i>	
Public-key cryptosystem based on the discrete logarithm problem	469
<i>L. Harn (University of Missouri-Kansas, USA),</i>	
<i>S. Yang (University of Science and Technology of China, PRC)</i>	

Session 12: PUBLIC KEY CRYPTOGRAPHY II

Chair: John Snare

Elliptic curves over F_p suitable for cryptosystems	479
<i>A. Miyaji (Matsushita Electric Industrial Co. LTD., Japan)</i>	
The probability distribution of the Diffie-Hellman key	492
<i>C.P. Waldvogel, J.L. Massey (Swiss Federal Institute of Technology, Switzerland)</i>	
A modular exponentiation unit based on systolic arrays	505
<i>J. Sauerbrey (Technische Universität München, Germany)</i>	
A comparison of key distribution patterns	
constructed from circle geometries	517
<i>C.M. O’Keefe (University of Adelaide, Australia)</i>	

Rump Session

Chair: Josef Pieprzyk

A block cipher method using combinations of different methods under the control of the user key	531
<i>M. Rezný, E. Trimarchi (Queensland University of Technology, Australia)</i>	
An attack on two hash functions by Zheng-Matsumoto-Imai	535
<i>B. Preneel, R. Govaerts, J. Vandewalle (Katholieke Universiteit Leuven, Belgium)</i>	
Primality testing with Lucas functions	539
<i>R. Lidl (University of Tasmania, Australia), W. B. Müller (Universität Klagenfurt, Austria)</i>	
Author Index	543

Session 1

**AUTHENTICATION AND SECRET
SHARING I**

Chair: Diane Donovan

(Queensland University of Technology, Australia)

Threshold Cryptosystems

Yvo Desmedt*

EE & CS Department, University of Wisconsin-
Milwaukee, WI 53201, U.S.A.

Abstract. Often the power to use a cryptosystem has to be shared. In threshold schemes, t -out-of- l have the power to regenerate a secret key (while less than t have not). However threshold schemes cannot be used directly in many applications, such as threshold signatures in which t -out-of- l have to co-sign a message. A normal threshold scheme would require the shareholders to send their shares to a trusted person who would sign for them. But the use of such a trusted person violates the main point of threshold signatures!

We first overview the research in the field and then discuss a threshold decryption/signature scheme which is as secure as RSA. We conclude by giving a list of open problems.

1 Introduction

1.1 The Concept and its Importance

In the classical mechanical example used to illustrate sharing two bank clerks are necessary to open the bank vault. While sharing schemes are useful for such control purposes, more is required when wholesale transactions are co-signed by two members of the bank. Indeed, when one requires that two bank clerks authorize (or sign) a large transaction (appending an authenticator), it is required that the authenticator is message dependent. The classical way to achieve this is to use first a sharing secret scheme which outputs the secret key. This secret key is then given to an authentication scheme. The first solution has the obvious disadvantage that each of the clerks knows the secret key and could perform (now or later) a fraud with it, *e.g.*, by authenticating a different message. In the second solution the shareholders transfer their complete power to a third party. A better solution would be that the bank clerks calculate the authenticator (or signature) all together such that above fraud is impossible, *i.e.*, while *not* divulging their shares. This last solution is precisely what *threshold authentication* (or signature) is about. In general, the goal of threshold cryptography is to design cryptosystems in which the power to perform a certain operation is shared. A further generalization is to allow that we have a more general access structure [29] than just a threshold.

The importance of threshold signature is clear when one considers that majority is often a threshold too and that in a democracy no member of the congress

* A part of this work has been supported by NSF Grant NCR-9106327.

(parliament) has the power himself to make a law, but that a majority is required. Even the concept of the president having a veto power can be included when using general access structures instead of threshold schemes.

Threshold cryptography can contribute in the fight against abuse of power by the government or any individual inside an organization. To give another illustration besides threshold signatures consider threshold decryption. In the United States a proposal that would allow the government to eavesdrop encrypted messages has been heavily debated [36, p. 46] and [11]. Micali [31] proposed to use threshold schemes to achieve this goal. In his scheme each user of a cryptosystem has to deposit shares of his secret key in banks and other respectful organizations. When a court order is provided shareholders are forced to reveal their shares to, let us say, the Federal Bureau of Investigation (FBI). A major disadvantage of his scheme is that once these shares have been provided to the FBI this organization could abuse the obtained secret key to decrypt any message, even those sent after the court order was successfully appealed. So once such a court order has been successfully appealed, the receiver has to publish a new public key. Threshold decryption allows for a scenario in which the court specifies which messages have to be decrypted. Under the assumption that no number of shareholders larger or equal than the threshold will ever become corrupt, threshold decryption allows a threshold of shareholders to decrypt specific messages without leaking during this process anything about other plaintexts or the secret key. So there is even no need to publish a new public key after a successful appeal.

Another important property of threshold cryptography is its reliability. This reliability is needed in many organizations that must provide their services (e.g., sign and validate documents) even when the head is on vacation or sick.

1.2 Its Origin

Let us now briefly overview the origin of threshold cryptography. The first threshold cryptosystems were independently developed by Boyd [3], Croft-Harris [8] and Desmedt [16].

A 2-out-of-1 RSA (signature) scheme [37] has been presented by Boyd [3]. It is not clear whether this scheme is as secure as RSA. Shares of the secret exponent d are given such that any two shareholders can sign a message. The final output is a normal RSA signature. So, to verify the signature an outsider does not need to know who the shareholders are. In this approach it is sufficient that all shareholders as a group have one public key and the shareholders themselves could be *anonymous*. Examples of such groups are organizations we are familiar with in our society, such as banks, companies, etc. The generation of the signature in this scheme is serial (one shareholder sends his partial result to the other to obtain the RSA signature).

A scheme for t -out-of-1 "authorizations" has been proposed by Croft and Harris [8]. They also attempted to present a threshold key exchange protocol. Their scheme uses a prime order subgroup of Z_p^* (predating [38]). Because the authorizations are independent of the message the scheme is insecure for many

applications. The threshold key exchange protocol suffers from a security bug (less than the threshold of shareholders can break the system).

The author introduced the concept of society oriented cryptography [16]. Sender and receiver are then organizations instead of individuals. The author described (what he would now call) threshold decryption, in which a threshold of shareholders are needed to decipher a message. To motivate the need for threshold decryption the author cites that in some modern software companies two supervisors are responsible for software developing projects. Continuity is then guaranteed when one of supervisors leaves — a not unlikely event in this business. Different problems are also introduced, many of which are still unsolved. The solution presented for threshold decryption (in which the threshold is 50%) is entirely based on mental games [24].

Although mental games can easily provide threshold cryptosystems they are unsatisfactory because modern implementations are completely impractical by requiring the shareholders to heavily interact. The *challenge* is the development of *non-interactive* threshold cryptosystems. In Section 2 we overview the results, achieved so far, in attaining this goal. Seen above we further ignore in our discussions solutions that need interaction between shareholders.

1.3 Definition

Let us avoid to be too formal. Instead we will focus on the essential aspects of threshold cryptography. Moreover readers for whom the examples above are sufficient to grasp the meaning of threshold cryptography can skip the rest of this section.

Let us suppose that we have a cryptosystem A which is used in a cryptographic protocol (A, R) , where R is a collection of machines, so that we have a robust (workable) and secure system. Let t and l be fixed integers. If we now replace the machine A by a collection of machines $A = (A_1, A_2, \dots, A_l, C)$ such that:

1. (*Reliability*) $\forall \{i_1, \dots, i_t\} \subset \{1, \dots, l\}$: the cryptographic protocol $((A_{i_1}, A_{i_2}, \dots, A_{i_t}, C), R)$, in which $(A_{i_1}, A_{i_2}, \dots, A_{i_t}, C)$ behave as an entity, satisfies the former robustness and security condition,
2. (*Threshold Security*) $\forall t' \leq t - 1 : \forall \{i_1, \dots, i_{t'}\} \subset \{1, \dots, l\} : (\tilde{A}_{i_1}, \tilde{A}_{i_2}, \dots, \tilde{A}_{i_{t'}}, \tilde{C})$ cannot give more power to an adversary by trying to help the adversary, where \tilde{A}_{i_j} private information (tape) is identical to the one of A_{i_j} and \tilde{A}_{i_j} has eavesdropped in previous executions of the scheme the output of each shareholder, where, in the case of unconditional security \tilde{A}_{i_j} and \tilde{C} are any machines, while for conditional Threshold Security their computer power is (polynomially) bounded,

then we call $(A_1, A_2, \dots, A_l, C)$ a t -out-of- l threshold cryptosystem. If A , used in the protocol (A, R) , has been called an S -system, then we call $(A_1, A_2, \dots, A_l, C)$ a threshold S -system.

To generalize the definition to include general sharing, we modify the Reliability Condition (1.) to require that $\{i_1, \dots, i_t\} \in \Gamma_{\{1, \dots, n\}}$ and we modify the Threshold Security Condition (2.) so that $\{i_1, \dots, i_t\} \notin \Gamma_{\{1, \dots, n\}}$, where $\Gamma_{\{1, \dots, n\}}$ is the access structure. We say that the entity A has *anonymous members* [16] if the machines R above do not "see" the difference between the execution of (A, R) and $((A_{i_1}, A_{i_2}, \dots, A_{i_t}, C), R)$. To achieve this "anonymity" C will perform the external communications with R , receiving "partial results" from $A_{i_1}, A_{i_2}, \dots, A_{i_t}$. We call C the *combiner*.

Threshold schemes could be considered to be special cases of threshold cryptography in which A 's output is equal to the key.

1.4 Background

We assume that the reader is familiar with the concept of threshold schemes [2, 39] and general sharing schemes [29] allowing a specific access structure to reconstruct a secret key. For a bibliography on sharing schemes consult [41].

An important tool in modern threshold cryptography is the concept of homomorphic sharing scheme [1]. Informally, a sharing scheme is homomorphic if the product of the shares is a share of the product of the secret keys (in general the first operator could be different from the second, moreover the product could be a sum for example). A homomorphic sharing scheme is composite [1] if revealing all the shares of the key $k_1 * k_2$ does not leak anything additional about (k_1, k_2) besides what $k_1 * k_2$ does. So a composite sharing scheme is "leak free".

2 Overview of Existing Schemes

We overview research on threshold cryptography and its generalization towards sharing cryptographic power in a general access structure setting. Papers on related topics are discussed jointly. (So, papers that are multi disciplinary will be cited more than once.) We do not rediscuss research already cited in Section 1.2. We avoid to discuss schemes that require internal interaction between the shareholders, to avoid overlap with mental games (secure distributed computation).

2.1 Threshold Decryption

In Sections 1.1 and 1.2 we already discussed two applications of threshold decryption.

A scheme allowing t -out-of- l shareholders to decrypt incoming ciphertexts encrypted by the El Gamal [19] public key encryption scheme has been presented by Frankel [20]. This was generalized towards t -out-of- l decryption of El Gamal type ciphertexts in [13]. The Threshold Security of this scheme is easy to prove. In other words it satisfies the requirement that whatever they attempt $t - 1$ shareholders cannot help an adversary to eavesdrop. So it is as secure as the original El Gamal scheme. Pedersen observed that there is no need for a trusted key distributor in these schemes [35].

t -out-of- l decryption of RSA [37] type ciphertexts has been presented in [14]. Lai and Harn [30] presented a shared decryption scheme based on RSA that generalizes the threshold to any access structure. For some access structures the shareholders need exponential computer power. The Threshold Security of both schemes seems heuristic, because it is not clear how to prove (or disprove) that $t - 1$ shareholders are of no help to an eavesdropper. For threshold decryption this problem has been solved in [21]. Because RSA is not a proven secure public key scheme, only the Threshold Security fact has been proven, evidently. We briefly discuss the scheme in further detail in Section 3. In [21] it has also been observed that using the general sharing scheme of Simmons-Jackson-Martin [42], as adapted in [22], it is easy to make shared (in the sense of a general access) decryption of RSA with proven Threshold Security. For some access structure Simmons-Jackson-Martin generates exponentially large shares, requiring those access structures to be excluded when the number of shareholders is not very small (otherwise the scheme is impractical, moreover it would require the shareholders a computer power that would allow them to break RSA anyway).

A proven secure public key threshold decryption scheme is presented in [9]. While all above schemes require that no shareholder will jam the computation (e.g., by outputting random) this restriction has been removed as far as possible.

All the above shared decryption schemes are for an anonymous membership scenario. Hwang [28] presented a discrete log based decryption scheme in which the sender knows the shareholders.

Clearly the security of all these schemes is conditional. Unconditionally secure threshold decryption is easy to achieve by combining the one-time-pad [43, 40] with any threshold (general sharing) scheme.

2.2 Threshold Pseudorandom

The generation of a pseudorandom string by a threshold of anonymous shareholders has been studied in [5, 9]. The first scheme is based on RSA, while the second is based on secure one way functions with homomorphic trapdoor (such as RSA).

2.3 Threshold Encryption

The concept of sharing the power to encrypt a message makes no sense in a public key context, but does for symmetric cryptosystems. De Santis, Desmedt, Frankel and Yung present a proven secure threshold encryption scheme in [9] which is based on a threshold pseudorandom generator.

Unconditionally secure threshold encryption is similar as decryption.

2.4 Threshold Authentication and Signatures

Unconditional Security Threshold generation of authenticators by a set with anonymous members has been discussed in [14] (for a variant see also [18]).

This has been extended to include general access structures in [12]. As demonstrated in [12], the shared generation of authenticators can be achieved using any composite sharing scheme [1]. It was also observed that the Simmons-Jackson-Martin [42] scheme, as adapted in [22], is a composite sharing scheme.

Threshold verification of user identifiers has been proposed in [10].

Signatures First we observe that threshold signatures are somewhat related to multisignatures (e.g., [33, 32]) and group signatures [7]. In multisignatures a multiple of individuals are all going to sign a message. One could consider multisignatures as t -out-of- l threshold signatures with known members, where l is not necessarily fixed. Group signatures could be viewed as 1-out-of- l threshold "signatures" with anonymous members in which the anonymity has a trapdoor. To avoid to be sidetracked we do no longer discuss multisignatures and group signatures.

The shared generation by anonymous members of an RSA signature was discussed in [14, 30, 21]. These schemes are very similar to the threshold (shared) RSA decryption, discussed in Section 2.1, and have similar security.

Harn and Yang [27] discussed the threshold generation by anonymous members of undeniable signatures [6].

De Santis, Desmedt, Frankel and Yung present a proven secure threshold signature scheme with anonymous members in [9].

In undeniable signatures verifiers need the help of the signer to verify the validity of the signature. Transferring this power to a threshold of known shareholders has been discussed in [34]. It is important to observe that although any threshold of shareholders can help in the verification, the reliability of this scheme is only average. The scheme, based on a zero-knowledge protocol (see also Section 2.5), requires that the shareholder's computer does not go down immediately after having giving an output, but remains up for a certain time. We call a scheme *very reliable* when one assumes that the number of shareholders that must be up is larger or equal than a certain threshold but the set could change dynamically at any moment during the execution of the external (the combiner with the receivers R) protocol. If the scheme under consideration requires no external interaction it is automatically very reliable. But the verification process in [34] requires external interaction and has only an average reliability.

Other Authentication Schemes A proven secure threshold authentication scheme with anonymous co-authenticators was presented in [14]. The underlying authentication scheme is an adaptation [15] of the Goldwasser-Micali-Rivest scheme [26]. While the authentication tree is no longer needed, a zero-knowledge protocol is used (see also Section 2.5). The scheme only provides average reliability.

2.5 Threshold zero-knowledge proofs

A zero-knowledge protocol in which a threshold of known provers prove the simultaneous discrete log has been proposed [34]. For the case that shareholders

are anonymous a threshold of shareholders can in perfect zero-knowledge prove the knowledge of a square root, as briefly explained in [14]. Using [4, 17] this protocol can easily be generalized to a whole class of zero-knowledge proofs for different languages, as we further explain in Appendix A. Both protocols have only an average reliability. How to achieve very reliable computationally zero-knowledge proofs with a threshold of provers is explained in [9].

3 Threshold RSA as Secure as RSA

To illustrate the concept of threshold cryptosystems and combiner, we now describe in more detail one threshold cryptosystem. Desmedt and Frankel announced in [14, p. 460] a t -out-of- l threshold RSA scheme as secure as RSA. We here overview this Frankel-Desmedt scheme. We omit all proofs, which are given in [21].

Let $P(z) = \sum_{j=0}^{Q-1} z^j$, where Q is a prime greater than or equal to $l+1$. Let $Z[u] \cong Z[z]/(P(z))$, i.e., the ring of integer polynomials modulo $P(z)$. Let the public identity of shareholder i be: $x_i = \sum_{j=0}^{i-1} u^j$. Finally let us define the function $F_0 : Z[u] \rightarrow Z; b_0 + b_1 u + \dots + b_{Q-2} u^{Q-2} \rightarrow b_0$.

Key Initialization The trusted key distributor²:

- Step 1** chooses $n = pq$ and e and d as described in the RSA algorithm and publishes the public key (e, n) of the organization,
- Step 2** chooses with uniform probability distribution a random polynomial $f(x)$ of degree $t-1$ over $Z_\gamma[u]$ such that $f(0) = d \bmod \gamma$ where $\gamma = [n^2/\lambda(n)] \cdot \lambda(n)$,
- Step 3** privately transmits to each co-signer i the share $K_i = f(x_i)$ evaluated in $Z_\gamma[u]$.

Observe that $[n^2/\lambda(n)] \cdot \lambda(n)$ is not revealed in the above protocol. So a shareholder considers K_i as belonging to $Z[u]$.

Co-Signing Assume that the set of co-signers B ($|B| = t$), who will co-sign, is known to all co-signers. Each shareholder $i \in B$:

- Step 0** precomputes in $Z[u]$ (so modulo $P(z)$) $\alpha_{i,B} = K_i \cdot y_{i,B}$ where

$$y_{i,B} = \prod_{\substack{j \in B \\ j \neq i}} \frac{(0 - x_j)}{(x_i - x_j)}$$

to obtain the integer $\alpha_{i,B} = F_0(\alpha_{i,B})$.

- Step 1** co-signs a (hashed) message M by sending $S_{M,i,B} = M^{\alpha_{i,B}}$ to the combiner, C .

² Using mental games only during the initialization phase there is no need for a key distributor when t is small enough.

The Combiner sends the message and the signature $S_M = \prod_{i \in B} S_{M,i,B} \bmod n$ to the receiver.

One demonstrates in [21] that after precomputation the scheme is roughly as efficient as RSA when $t < \log_2 n$. It is also proven that the scheme is Reliable and Threshold Secure, *i.e.*, as secure as RSA. A reader could object to call this scheme non-interactive. Indeed shareholders must know who is active (which set B will co-sign), which normally requires some interaction. This problem can be solved by combining the scheme with the homomorphic sharing scheme presented in [17], as is discussed in detail in [9].

4 Conclusion

We have discussed the purpose and the need of threshold cryptosystems. We have seen that a threshold scheme on itself does not provide the required security. Our overview has demonstrated that this area has attracted a lot of research. While secure distributed computation has a more general scope (for an overview consult [23]), many of these schemes are not practical. Threshold cryptography is primarily interested in non-interactive solutions. Moreover, to be as realistic as possible, many schemes do not require that shareholders send in a given order their output to the combiner.

The attentive reader can see that some cryptosystems have no threshold equivalent yet. For example no threshold perfect zero-knowledge proof for graph isomorphism has been presented so far. Moreover no non-interactive threshold generation of DSS signatures has been found. May be some of these open problems can be proven to have no non-interactive solution. Other open problems are to improve the performance of many schemes and/or to prove their limitations. Although many threshold cryptosystems are based on some homomorphic property it has not been proven that such a property is necessary to achieve non-interactive threshold cryptosystems.

A Threshold zero-knowledge proofs

We sketch how to generalize the threshold zero-knowledge proof of [14].

We follow the notations of [4]. So let us briefly overview it. To simplify the discussion we focus on the case that $\mathcal{G} = \mathcal{G}' = \mathcal{G}''$ is an Abelian group (although some zero-knowledge protocols do not satisfy exactly this description they can trivially be modified to fit it). To have easy notations we assume $m = 1$. f is homomorphism and $f(\mathcal{G}) = \mathcal{H} \subset \mathcal{H}'$. $I \in \mathcal{H}$ is the "public number" which is a part of the input x and the "secret number" S belongs to a set \mathcal{G} .

The protocol in which A is the prover and R the verifier, is as follows: First the verifier checks that $I \in \mathcal{H}'$. Then repeat sufficiently many times:

Step 1 A selects a random $X \in \mathcal{G}$ and sends R : $Z = f(X)$ (A 's cover).

Step 2 R sends A a random $q \in \mathcal{Q}$ (R 's query).

Step 3 When $q \in \mathcal{Q}$, A sends R : $Y = X \cdot S^q$ (A 's answer).

Step 4 R verifies that $Y \in \mathcal{G}$ and that $f(Y) = Z \cdot I^q$ (R 's verification).

We now assume that multiplying and calculating inverses in $G(\cdot)$ can be done in polynomial time and that G is sampleable.

Let us introduce the reader to techniques we use. In zero-knowledge sharing schemes [17] the (view of the) key distribution phase can be simulated [25]. All *existing* homomorphic sharing schemes have the property that the key $k \in G$ can be written as:

$$k = \prod_{i \in B} \psi_{i,B}(s_i), \quad (1)$$

where B is in the access structure, s_i is i 's share, and $\psi_{i,B}$ is a function from the set from which i 's shares are chosen to G . When a sharing scheme satisfies (1) we call it *multiplicative*. It was proven [22] that when the set of keys is an Abelian group all ideal homomorphic sharing schemes are multiplicative. (It is an open problem whether any non-ideal homomorphic sharing scheme is multiplicative.) So, the homomorphic schemes of [17] for $G(\cdot)$ being any Abelian group are multiplicative, because they are ideal for a superset of G . Moreover they are zero-knowledge. Also the Simmons-Jackson-Martin [42] general sharing scheme, as adapted in [22], is multiplicative if $G(\cdot)$ is an Abelian group. If the shares are polynomially bounded it is also a zero-knowledge sharing scheme.

We now present the generalization. We assume that the set of co-provers B involved in the proof is in the access structure and is known to all co-provers. For a zero-knowledge interactive proof which can be described as above we explain how to modify it to obtain a zero-knowledge scheme with shared provers. We assume that a key distributor has given each shareholder its share s_i of the secret key S using a zero-knowledge multiplicative sharing scheme. Replace Steps 1–3 by:

- Step 1** Each shareholder $i \in B$ selects a random $X_i \in \mathcal{G}$ and sends: $Z_i = f(X_i)$ to C , the combiner. C calculates $Z = \prod_{i \in B} Z_i$ and sends Z to R .
- Step 2** R sends C a random $q \in Q$ which C broadcasts to all shareholders.
- Step 3** When $q \in Q$, each shareholder $i \in B$ sends C : $Y_i = X_i \cdot (\psi_{i,B}(s_i))^q$. Then C calculates $Y = \prod_{i \in B} Y_i$ and sends it to R .

The resulting protocol has the Threshold Security property. In other words, the joint view of $B \cup \{C\} \cup \{R\}$, where B is *not* in the access structure, is simulatable (approximable). As in Section 3 the reader could object to call this scheme non-interactive, because shareholders must know who is active. This can easily be solved when the Simmons-Jackson-Martin [42] general sharing scheme as adapted in [22] is used. It can also be solved using [17] based on a similar technique as in [9].

References

1. Benaloh, J. C.: Secret sharing homomorphisms: Keeping shares of a secret secret. In *Advances in Cryptology, Proc. of Crypto '86* (Lecture Notes in Computer Science 263) (1987) A. Odlyzko, Ed. Springer-Verlag pp. 251–260