Preface

The Information Security Conference 2001 brought together individuals involved in multiple disciplines of information security to foster the exchange of ideas. The conference, an outgrowth of the Information Security Workshop (ISW) series, was held in Málaga, Spain, on October 1–3, 2001. Previous workshops were ISW '97 at Ishikawa, Japan; ISW '99 at Kuala Lumpur, Malaysia; and ISW 2000 at Wollongong, Australia. The General Co-chairs, Javier López and Eiji Okamoto, oversaw the local organization, registration, and performed many other tasks.

Many individuals deserve thanks for their contribution to the success of the conference. José M. Troya was the Conference Chair. The General Co-chairs were assisted with local arrangements by Antonio Maña, Carlos Maraval, Juan J. Ortega, José M. Sierra, and Miguel Soriano.

This was the first year that the conference accepted electronic submissions. Many thanks to Dawn Gibson for assisting in developing and maintaining the electronic submission servers. The conference received 98 submissions of which 37 papers were accepted for presentation. These proceedings contain revised versions of the accepted papers. Revisions were not checked and the authors bear full responsibility for the contents of their papers.

The Program Committee consisted of Elisa Bertino, Università di Milano; G. R. Blakely, Texas A&M University; John Daugman, Cambridge University; Jorge Dávila, Polytechnic Univ. of Madrid; Giovanni DiCrescenzo, Telcordia; Josep Domingo-Ferrer, Univ. Rovira i Virgili; Dieter Gollmann, Microsoft Research; Sigrid Guergens, GMD; Hiroaki Kikuchi, Tokai University; Chi-Sung Laih, Natl. Cheng Kung Univ.; Wenbo Mao, HP Laboratories; Masahiro Mambo, Tohoku University; Catherine Meadows, NRL; Sang-Jae Moon, Kyungpook Natl. University; Yuko Murayama, Iwate Prefectural University; René Peralta, Yale University; Josef Pieprzyk, University of Wollongong; Sihan Qing, Chinese Academy of Sciences; Susie Thomson, Datacard; Routo Terada, Univ. of S. Paulo; Yiannis Tsiounis, InternetCash; Moti Yung, Certco; Yuliang Zheng, Monash University; Jianying Zhou, Oracle Corp. Members of the committee spent numerous hours in reviewing papers and providing advice. The committee was also assisted by our colleagues: Marc Alba, Clemente Galdi, Sang-Wook Kim, Yi Mu, Anna Oganian, Francesc Sebé, Rajan Shankaran, Igor Shparlinski. We apologize for any inadvertent omissions. Our thanks to the program committee and all reviewers.

We thank all the authors who submitted papers to this conference. Without their submissions this conference could not have been a success.

July 2001

George I. Davida
Yair Frankel
Information Security Conference 2001
October 1–3, 2001, Málaga, Spain

Conference Chair
José M. Troya, University of Málaga (Spain)

General Co-chairs
Javier López, University of Málaga (Spain)
Eiji Okamoto, Toho University (Japan)

Program Co-chair
George I. Davida, University of Wisconsin-Milwaukee (USA)
Yair Frankel, TechTegrity L.L.C. (USA)

Program Committee
Elisa Bertino .......................................................... Università di Milano (Italy)
G. R. Blakely.......................................................... Texas A&M University (USA)
John Daugman .......................................................... Cambridge University (UK)
Jorge Dávila .............................................................. Polytechnic Univ. of Madrid (Spain)
Giovanni DiCrescenzo ................................................... Telcordia (USA)
Josep Domingo-Ferrer ................................................. Univ. Rovira i Virgili (Spain)
Dieter Gollmann ........................................................ Microsoft Research (UK)
Sigrid Guergens ....................................................... GMD (Germany)
Hiroaki Kikuchi .......................................................... Tokyo University (Japan)
Chi-Sung Laih .......................................................... N.C. Cheng Kung Univ. (Taiwan)
Wenbo Mao ........................................................... HP Laboratories (UK)
Masahiro Mambo ........................................................ Tohoku University (Japan)
Catherine Meadows ..................................................... NRL (USA)
Sang-Jae Moon ........................................................ Kyungpook Natl. University (Korea)
Yuko Murayama ....................................................... Iwate Prefectural University (Japan)
Rene Peralta ............................................................. Yale University (USA)
Josef Pieprzyk ........................................................ University of Wollongong (Australia)
Sihan Qing ............................................................. Chinese Academy of Sciences (China)
Susie Thomson ........................................................ Datacard (UK)
Routo Terada ......................................................... Univ. of S. Paulo (Brazil)
Yiannis Tsiounis ........................................................ InternetCash (USA)
Moti Yung ............................................................... CertCo (USA)
Yuliang Zheng ........................................................ Monash University (Australia)
Jianying Zhou ........................................................ Oracle Corp. (USA)
# Table of Contents

## Key Distribution

Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures .................. 1  
**Carlo Blundo, Paolo D'Arco (Università di Salerno)**  
**Vanesa Daza, and Carles Padró (Universitat Politècnica de Catalunya)**  

Privacy Amplification Theorem for Noisy Main Channel ........................................ 18  
**Valeri Korjik, Guillermo Morales-Luna (CINVESTAV-IPN),**  
**and Vladimir B. Balakirsky (EIDMA)**  

## Protocols

Efficient Kerberized Multicast in a Practical Distributed Setting......................... 27  
**Giovanni Di Crescenzo (Telcordia Technologies)**  
**and Olga Kornievskaia (University of Michigan)**  

Suitability of a Classical Analysis Method for E-commerce Protocols.............. 46  
**Sigrid Gürgens (GMD-SIT) and Javier Lopez (University of Malaga)**  

## Enhancing Technologies

Hyppocrates (A New Proactive Password Checker) ........................................ 63  
**Carlo Blundo, Paolo D'Arco, Alfredo De Santis,**  
**and Clemente Galdi (Università di Salerno)**  

Lenient/Strict Batch Verification in Several Groups......................................... 81  
**Fumitaka Hoshino, Masayuki Abe,**  
**and Tetsutaro Kobayashi (NTT Corporation)**  

## Privacy

Absolute Privacy in Voting .................................................................................. 95  
**Dmitri Asonov (Humboldt-Universität zu Berlin),**  
**Markus Schaal (Technische Universität Berlin), and**  
**Johann-Christoph Freytag (Humboldt-Universität zu Berlin)**  

A Logical Model for Privacy Protection ............................................................... 110  
**Tsan-sheng Hsu, Churn-Jung Liau,**  
**and Da-Wei Wang (Academia Sinica)**
**Software Protection**

DISSECT: DIStribution for SECurity Tool ........................................................... 125  
*Enriquillo Valdez* (Polytechnic University of New York)  
and *Moti Yung* (CertCo, Inc.)

An Approach to the Obfuscation of Control-Flow  
of Sequential Computer Programs ................................................................. 144  
*Stanley Chow, Yuan Gu, Harold Johnson* (Cloakware Corporation),  
and *Vladimir A. Zakharov* (Moscow State University)

**Message Hiding I**

A Practical and Effective Approach to Large-Scale Automated  
Linguistic Steganography ..................................................................................... 156  
*Mark Chapman* (Omni Tech Corp.),  
*George I. Davida* (University of Wisconsin-Milwaukee), and  
*Marc Rennhard* (Swiss Federal Institute of Technology)

Robust New Method in Frequency Domain Watermarking ............................... 166  
*David Sánchez, Agustín Orfila, Julio César Hernández,*  
and *José María Sierra* (Carlos III University)

**PKI Issues and Protocols**

On the Complexity of Public-Key Certificate Validation .............................. 183  
*Diana Berbecaru, Antonio Lioy,* and  
*Marius Marian* (Politecnico di Torino)

Liability of Certification Authorities: A Juridical Point of View ................... 204  
*Apol·lònia Martínez-Nadal* and  
*Josep L. Ferrer-Gomila* (Universitat de les Illes Balears)

**Hardware Implementations**

Experimental Testing of the Gigabit IPSec-Compliant Implementations of  
Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board .............. 220  
*Pawel Chodowiec, Kris Gaj* (George Mason University),  
*Peter Bellows,* and *Brian Schott* (University of Southern California)

Elliptic Curve Arithmetic Using SIMD ............................................................ 235  
*Kazumaro Aoki* (NTT Communications), *Fumitaka Hoshino,*  
*Tetsutaro Kobayashi,* and *Hiroaki Oguro* (NTT Corporation)
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>On the Hardware Implementation of the 3GPP Confidentiality and Integrity Algorithms</td>
<td>248</td>
</tr>
<tr>
<td>Kostas Marinis (National Technical University of Athens), Nikos K. Moshopoulos, F. Karoubalis (Atmel Hellas), and Kiamal Z. Pekmestzi (National Technical University of Athens)</td>
<td></td>
</tr>
<tr>
<td>Efficient Implementation of Elliptic Curve Cryptosystems on an ARM7 with Hardware Accelerator</td>
<td>266</td>
</tr>
<tr>
<td>Sheng-Bo Xu and Lejla Batina (Securealnk B.V.)</td>
<td></td>
</tr>
<tr>
<td>Cryptanalysis and Prevention</td>
<td></td>
</tr>
<tr>
<td>A Theoretical DPA-Based Cryptanalysis of the NESSIE Candidates FLASH and SFLASH</td>
<td>280</td>
</tr>
<tr>
<td>Rainer Steinwandt, Willi Geiselmann, and Thomas Beth (Universität Karlsruhe)</td>
<td></td>
</tr>
<tr>
<td>Quadratic Relations for S-Boxes: Their Minimum Representations and Bounds</td>
<td>294</td>
</tr>
<tr>
<td>Routo Terada and Paulo G. Pinheiro (University of S. Paulo)</td>
<td></td>
</tr>
<tr>
<td>Approximate Power Roots in $\mathbb{Z}_m$</td>
<td>310</td>
</tr>
<tr>
<td>Ismael Jiménez-Calvo (C.S.I.C.) and German Sáez-Moreno (Universitat Politècnica de Catalunya)</td>
<td></td>
</tr>
<tr>
<td>Securing Elliptic Curve Point Multiplication against Side-Channel Attacks</td>
<td>324</td>
</tr>
<tr>
<td>Bodo Möller (Technische Universität Darmstadt)</td>
<td></td>
</tr>
<tr>
<td>Implementations</td>
<td></td>
</tr>
<tr>
<td>A Flexible Role-Based Access Control Model for Multimedia Medical Image Database Systems</td>
<td>335</td>
</tr>
<tr>
<td>Sofia Tzelepi and George Pangalos (Aristotelian University)</td>
<td></td>
</tr>
<tr>
<td>A Secure Publishing Service for Digital Libraries of XML Documents</td>
<td>347</td>
</tr>
<tr>
<td>Elisa Bertino, Barbara Carminati (Università di Milano), and Elena Ferrari (Università dell’Insubria)</td>
<td></td>
</tr>
<tr>
<td>Non-repudiation Techniques</td>
<td></td>
</tr>
<tr>
<td>An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party</td>
<td>363</td>
</tr>
<tr>
<td>Olivier Markowitch and Steve Kremer (Université Libre de Bruxelles)</td>
<td></td>
</tr>
</tbody>
</table>
Persistent Authenticated Dictionaries and Their Applications ......................... 379
Aris Anagnostopoulos (Brown University),
Michael T. Goodrich (University of California), and
Roberto Tamassia (Brown University)

Contracts and Auctions

Efficient Optimistic N-Party Contract Signing Protocol .................................... 394
Josep L. Ferrer-Gomila, Magadalena Payeras-Capellà,
and Llorenç Huguet-Rotger (Universitat de les Illes Balears)

Efficient Sealed-Bid Auctions for Massive Numbers of Bidders
with Lump Comparison ..................................................................................... 408
Koji Chida, Kunio Kobayashi,
and Hikaru Morita (NTT Corporation)

Message Hiding II

Oblivious Image Watermarking Robust against Scaling and Geometric Distortions
Francesc Sebé and Josep Domingo-Ferrer (Universitat Rovira i Virgili)

Fingerprinting Text in Logical Markup Languages ........................................ 433
Christian D. Jensen (Trinity College Dublin)

Payments

SPEED Protocol: Smartcard-Based Payment with Encrypted Electronic Delivery ........................................................................................................... 446
Antonio Ruiz, Gregorio Martínez, Oscar Cánovas,
and Antonio F. Gómez (University of Murcia)

Efficient Transferable Cash with Group Signatures ......................................... 462
Ik Rae Jeong, Dong Hoon Lee,
and Jong In Lim (Korea University)

Security Applications

An Auditable Metering Scheme for Web Advertisement Applications .......... 475
Liqun Chen and Wenbo Mao (Hewlett-Packard Laboratories)
Broker-Based Secure Negotiation of Intellectual Property Rights .......................... 486
Jaime Delgado (Universitat Pompeu Fabra), Isabel Gallego
(Universitat Politècnica de Catalunya), and Xavier Perramon
(Universitat Pompeu Fabra)

Network and OS Security

Design of the Decision Support System for Network Security
Management to Secure Enterprise Network .......................................................... 497
Jae Seung Lee (ETRI) and
Sang Choon Kim (Samchok National University)

Measuring False-Positive by Automated Real-Time Correlated Hacking
Behavior Analysis ................................................................................................. 512
Jia Wang and Insup Lee (University of Pennsylvania)

Design of UNIX System for the Prevention of Damage Propagation
by Intrusion and Its Implementation Based on 4.4BSD .............................................. 536
Kenji Masui, Masahiko Tomoishi,
and Naoki Yonezaki (Tokyo Institute of Technology)

Author Index ........................................................................................................ 553