Preface

The third International Workshop on Information Security was held at the University of Wollongong, Australia. The conference was sponsored by the Centre for Computer Security Research, University of Wollongong. The main themes of the conference were the newly emerging issues of Information Security. Multimedia copyright protection and security aspects of e-commerce were two topics that clearly reflect the focus of the conference. Protection of the copyright of electronic documents seems to be driven by strong practical demand from the industry for new, efficient and secure solutions. Although e-commerce is already booming, it has not reached its full potential in terms of new, efficient and secure e-commerce protocols with added properties.

There were 63 papers submitted to the conference. The program committee accepted 23. Of those accepted, six papers were from Australia, five from Japan, two each from Spain, Germany and the USA, and one each from Finland and Sweden. Four papers were co-authored by international teams from Canada and China, Korea and Australia, Taiwan and Australia, and Belgium, France and Germany, respectively.

Final versions of the accepted papers were gathered using computing and other resources of the Institute of Mathematics, Polish Academy of Sciences, Warsaw, Poland. We are especially grateful to Jerzy Urbanowicz and Andrzej Pokrzywa for their help during preparation of the proceedings.

We would like to thank the members of the program committee who gave generously of their time to read and evaluate papers. We would also like to thank members of the organising committee. Finally we thank the authors of all the submitted papers, in particular the accepted ones, and all the participants who contributed to the success of the conference.

October 2000

Josef Pieprzyk
Eiji Okamoto
Jennifer Seberry
THIRD INFORMATION SECURITY WORKSHOP
ISW2000

Sponsored by
Center for Computer Security Research
University of Wollongong, Australia

General Chair:
Jennifer Seberry
University of Wollongong, Australia

Program Co-chairs:
Josef Pieprzyk
University of Wollongong, Australia
Eiji Okamoto
University of Wisconsin-Milwaukee, USA

Program Committee:
George Davida
University of Wisconsin-Milwaukee, USA
Josep Domingo-Ferrer
University of Rovira i Virgili, Spain
Ed Dawson
Queensland University of Technology, Australia
Thomas Hardjono
Nortel Networks, USA
Hiroaki Kikuchi
Tokai University, Japan
Masahiro Mambo
Tohoku University, Japan
Yi Mu
Western Sydney University, Australia
Fabien Petitcolas
Microsoft Research, UK
Vijay Varadharajan
Western Sydney University, Australia
Yuliang Zheng
Monash University, Australia

Referees:
Marc Alba
Goichiro Hanaoka
Patrick Loo
Jordi Castellá
Thomas Hardjono
Masahiro Mambo
Ed Dawson
J. Herrera-Joancomartí
Kenta Matsuura
Josep Domingo-Ferrer
Stefan Katzenbeisser
Yi Mu
Cédric Fournet
Hiroaki Kikuchi
Yuko SJ Murayama
Dieter Gollmann
Helger Lipmaa
Kenny Nguyen
## VIII Organization

<table>
<thead>
<tr>
<th>Khanh Quoc Nguyen</th>
<th>Fabien Petitcolas</th>
<th>Mitsuru Tada</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ryutarou Ohbuchi</td>
<td>Josef Pieprzyk</td>
<td>Yuji Watanabe</td>
</tr>
<tr>
<td>Eiji Okamoto</td>
<td>Michael Roe</td>
<td>Bennet Yee</td>
</tr>
<tr>
<td>Adrian Perrig</td>
<td>Francesc Sebé</td>
<td>Yuliang Zheng</td>
</tr>
</tbody>
</table>
Table of Contents

Multimedia Copyright Protection

A Watermarking Scheme Based on the Characteristic of Addition among DCT Coefficients
Minoru Kuribayashi and Hatsukazu Tanaka ...................................................... 1

Affine Invariant Watermarks for 3D Polygonal and NURBS Based Models
Oliver Benedens .......................................................... 15

A Steganographic Framework for Reference Colour Based Encoding and Cover Image Selection
René Rosenbaum and Heidrun Schumann ........................................ 30

Spatial-Domain Image Watermarking Robust against Compression, Filtering, Cropping, and Scaling
Francesc Sebé, Josep Domingo-Ferrer, and Jordi Herrera ................... 44

Region-Based Watermarking by Distribution Adjustment
Gareth Brisbane, Rei Safavi-Naini, and Philip Ogunbona ................... 54

Hiding Information in Color Images Using Small Color Palettes
Tapio Seppänen, Kaisu Mäkelä, and Anja Keskinarkaus ....................... 60

An Approach to the Objective and Quantitative Evaluation of Tamper-Resistant Software
Hideaki Goto, Masahiro Mambo, Kenjiro Matsumura, and Hiroki Shizuya ... 82

Characteristics of Some Binary Codes for Fingerprinting
Tina Lindkvist .............................................................. 97

E-Commerce

An Anonymous Auction Protocol with a Single Non-trusted Center
Using Binary Trees
Kazumasa Omote and Atsuko Miyaji .................................................. 108

Unlinkable Divisible Electronic Cash
Toru Nakanishi and Yuji Sugiyama .................................................. 121

Weighted One-Way Hash Chain and Its Applications
Sung-Ming Yen and Yuliang Zheng ............................................... 135

Linkability in Practical Electronic Cash Design
Greg Maitland, Jason Reid, Ernest Foo, Colin Boyd, and Ed Dawson ...... 149
Towards a Practical Secure Framework for Mobile Code Commerce  
Gaël Hachez, Laurent Den Hollander, Mehrdad Jalali, Jean-Jacques Quisquater, and Christophe Vasserot ........................164

Key Management

Probabilistic Methods in Multicast Key Management  
Ali Aygün Selçuk and Deepinder Sidhu .............................179

Classification of Authentication Protocols: A Practical Approach  
DongGook Park, Colin Boyd, and Ed Dawson .........................194

Exploring Fair Exchange Protocols Using Specification Animation  
Colin Boyd and Peter Kearney ........................................209

A Practical Implementation of Hierarchically Structured Key Predistribution System and Its Evaluation  
Daisuke Nojiri, Goichiro Hanaoka, and Hideki Imai ..........................224

Network Security and Access Control

An Efficient Protocol for Certified Electronic Mail  
Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, and Llorenç Huguet i Rotger ........................................................237

Performance Analysis of Secure Web Server Based on SSL  
Xiaodong Lin, Johnny W. Wong, and Weidong Kou .....................249

Sherlock: Commercial High Assurance Network Computing  
Stephen P. Morgan, Stephen W. Neal, Melissa A. Hartman, and Matthew R. Laue ..........................................................262

The Role of the Development Process in Operating System Security  
Christian Payne .................................................................277

Cryptographic Systems

Threshold Fail-Stop Signature Schemes Based on Discrete Logarithm and Factorization  
Rei Safavi-Naini and Willy Susilo ........................................292

A Signcryption Scheme Based on Integer Factorization  
Ron Steinfeld and Yuliang Zheng ........................................308

Author Index .................................................................323