
CONTENTS

Keynote Speech

International Cryptography	1
<i>Doug McGowan</i>	

Cryptanalysis

Reaction attacks against several public key cryptosystems	2
<i>C. Hall, I. Goldberg, and B. Schneier</i>	

Cryptanalysis of some AES candidate algorithms	13
<i>W. Wu, B. Li, D. Feng, and S. Qing</i>	

Language Based Approach to Security

Issues in the design of a language for role based access control	22
<i>M. Hitchens and V. Varadharajan</i>	

Extending Erlang for safe mobile code execution	39
<i>L. Brown and D. Sahlin</i>	

Electronic Commerce and Secret Sharing

Detachable electronic coins	54
<i>C. Pavlovski, C. Boyd, and E. Foo</i>	

Linear secret sharing with divisible shares	71
<i>J. Pieprzyk</i>	

Efficient publicly verifiable secret sharing schemes with fast or delayed recovery	87
<i>F. Boudot and J. Traoré</i>	

Digital Signatures

Zero-knowledge proofs of possession of ElGamal-like digital signatures and its applications	103
<i>K. Q. Nguyen, F. Bao, Y. Mu, and V. Varadharajan</i>	

Signature scheme for controlled environments	119
<i>K. Viswanathan, C. Boyd, and E. Dawson</i>	

On the cryptographic value of the Qth root problem	135
<i>C. L. Beaver, P. S. Gemmell, A. M. Johnston, and W. Neumann</i>	

Keynote Speech

Protecting Critical Information Systems 143
Sushil Jajodia

Security Protocols

Delegation chains secure up to constant length 144
M. Abe and T. Okamoto

Optimal construction of unconditionally secured ID-based key
sharing scheme for large-scale networks 157
G. Hanaoka, T. Nishioaka, Y. Zheng, and H. Imai

Enhancing the resistance of a provably secure key agreement protocol to
a denial-of-service attack 169
S. Hirose and K. Matsuura

An extended logic for analyzing timed-release public-key protocols 183
M. Kudo and A. Mathuria

Applications

Bringing together X.509 and EDIFACT public key
infrastructures: The DEDICA project 199
M. Rubia, J. C. Cruellas, and M. Medina

User identification system based on biometrics for keystroke 216
K. Omote and E. Okamoto

Boundary conditions that influence decisions about log file formats
in multi-application smart cards 230
C. Markantonakis

Sending message into a definite future 244
W. Mao

Cryptography

Efficient accumulators without trapdoor 252
T. Sander

Evolutionary heuristics for finding cryptographically strong S-Boxes 263
W. Millan, L. Burnett, G. Garter, A. Clark, and E. Dawson

Incremental authentication of tree-structured documents 275
P. Ekdahl and B. Smeets

Complexity and Security Functions

Plateaued Functions 284
Y. Zheng and X.-M. Zhang

On the linear complexity of the Naor-Reingold pseudo-random function ...	301
<i>F. Griffin and I. E. Shparlinski</i>	
On the channel capacity of narrow-band subliminal channels	309
<i>K. Kobara and H. Imai</i>	
Author Index	325

Information and Communication Security
Second International Conference, ICICS'99 Sydney,
Australia, November 9-11, 1999 Proceedings
Varadharajan, V.; Mu, Y. (Eds.)
1999, XII, 328 p., Softcover
ISBN: 978-3-540-66682-0