

Table of Contents

Stream Ciphers and Boolean Functions

The Correlation of a Boolean Function with Its Variables	1
<i>Dingyi Pei and Wenliang Qin</i>	
On Choice of Connection-Polynomials for LFSR-Based Stream Ciphers . . .	9
<i>Jambunathan K</i>	
On Resilient Boolean Functions with Maximal Possible Nonlinearity	19
<i>Yuriy V. Tarannikov</i>	

Cryptanalysis I : Stream Ciphers

Decimation Attack of Stream Ciphers	31
<i>Eric Filiol</i>	
Cryptanalysis of the A5/1 GSM Stream Cipher	43
<i>Eli Biham and Orr Dunkelman</i>	

Cryptanalysis II : Block Ciphers

On Bias Estimation in Linear Cryptanalysis	52
<i>Ali Aydın Selçuk</i>	
On the Incomparability of Entropy and Marginal Guesswork in Brute-Force Attacks	67
<i>John O. Pliam</i>	
Improved Impossible Differentials on Twofish	80
<i>Eli Biham and Vladimir Furman</i>	

Electronic Cash & Multiparty Computation

An Online, Transferable E-Cash Payment System	93
<i>R. Sai Anand and C.E. Veni Madhavan</i>	
Anonymity Control in Multi-bank E-Cash System	104
<i>Ik Rae Jeong and Dong Hoon Lee</i>	
Efficient Asynchronous Secure Multiparty Distributed Computation	117
<i>K. Srinathan and C. Pandu Rangan</i>	
Tolerating Generalized Mobile Adversaries in Secure Multiparty Computation	130
<i>K. Srinathan and C. Pandu Rangan</i>	

Digital Signatures

Codes Identifying Bad Signatures in Batches	143
<i>Jarostaw Pastuszak, Josef Pieprzyk and Jennifer Seberry</i>	
Distributed Signcryption	155
<i>Yi Mu and Vijay Varadharajan</i>	
Fail-Stop Signature for Long Messages	165
<i>Rei Safavi-Naini, Willy Susilo and Huaxiong Wang</i>	

Elliptic Curves

Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack	178
<i>Katsuyuki Okeya and Kouichi Sakurai</i>	
Efficient Construction of Cryptographically Strong Elliptic Curves	191
<i>Johannes Buchmann and Harald Baier</i>	

Fast Arithmetic

High-Speed Software Multiplication in F_{2^m}	203
<i>Julio López and Ricardo Dahab</i>	
On Efficient Normal Basis Multiplication	213
<i>A. Reyhani-Masoleh and M. A. Hasan</i>	

Cryptographic Protocols

Symmetrically Private Information Retrieval	225
<i>Sanjeev Kumar Mishra and Palash Sarkar</i>	
Two-Pass Authenticated Key Agreement Protocol with Key Confirmation .	237
<i>Boyeon Song and Kwangjo Kim</i>	
Anonymous Traceability Schemes with Unconditional Security	250
<i>Reihaneh Safavi-Naini and Yejing Wang</i>	

Block Ciphers & Public Key Cryptography

New Block Cipher DONUT Using Pairwise Perfect Decorrelation	262
<i>Dong Hyeon Cheon, Sang Jin Lee, Jong In Lim and Sung Jae Lee</i>	
Generating RSA Keys on a Handheld Using an Untrusted Server	271
<i>Dan Boneh, Nagendra Modadugu and Michael Kim</i>	
A Generalized Takagi-Cryptosystem with a modulus of the form $p^r q^s$	283
<i>Seongan Lim, Seungjoo Kim, Ikkwon Yie and Hongsub Lee</i>	
Author Index	295

Progress in Cryptology - INDOCRYPT 2000

First International Conference in Cryptology in India,
Calcutta, India, December 10-13, 2000. Proceedings

Roy, B.; Okamoto, E. (Eds.)

2000, X, 302 p., Softcover

ISBN: 978-3-540-41452-0