

Table of Contents

Elliptic Curve Enhancements

Modifications of ECDSA	1
<i>John Malone-Lee and Nigel P. Smart</i>	

Integer Decomposition for Fast Scalar Multiplication on Elliptic Curves . .	13
<i>Dongryeol Kim and Seongan Lim</i>	

Analysis of the Gallant-Lambert-Vanstone Method Based on Efficient Endomorphisms: Elliptic and Hyperelliptic Curves	21
<i>Francesco Sica, Mathieu Ciet, and Jean-Jacques Quisquater</i>	

SNOW

Guess-and-Determine Attacks on SNOW	37
<i>Philip Hawkes and Gregory G. Rose</i>	

A New Version of the Stream Cipher SNOW	47
<i>Patrik Ekdahl and Thomas Johansson</i>	

Encryption Schemes

Encryption-Scheme Security in the Presence of Key-Dependent Messages .	62
<i>John Black, Phillip Rogaway, and Thomas Shrimpton</i>	

On the Security of CTR + CBC-MAC	76
<i>Jakob Jonsson</i>	

Single-Path Authenticated-Encryption Scheme Based on Universal Hashing	94
<i>Soichi Furuya and Kouichi Sakurai</i>	

Differential Attacks

Markov Truncated Differential Cryptanalysis of Skipjack	110
<i>Ben Reichardt and David Wagner</i>	

Higher Order Differential Attack of <i>Camellia</i> (II)	129
<i>Yasuo Hatano, Hiroki Sekine, and Toshinobu Kaneko</i>	

Square-like Attacks on Reduced Rounds of IDEA	147
<i>Hüseyin Demirci</i>	

Full-Round Differential Attack on the Original Version of the Hash
Function Proposed at PKC'98 160
*Donghoon Chang, Jaechul Sung, Soohak Sung, Sangjin Lee, and
Jongin Lim*

Boolean Functions and Stream Ciphers

On Propagation Characteristics of Resilient Functions 175
Pascale Charpin and Enes Pasalic

Two Alerts for Design of Certain Stream Ciphers: Trapped LFSR and
Weak Resilient Function over $GF(q)$ 196
Paul Camion, Miodrag J. Mihaljević, and Hideki Imai

Multiples of Primitive Polynomials and Their Products over $GF(2)$ 214
Subhamoy Maitra, Kishan Chand Gupta, and Ayineedi Venkateswarlu

A New Cryptanalytic Attack for PN-generators Filtered by a Boolean
Function 232
Sabine Leveiller, Gilles Zémor, Philippe Guillot, and Joseph Boutros

Block Cipher Security

White-Box Cryptography and an AES Implementation 250
*Stanley Chow, Philip Eisen, Harold Johnson, and
Paul C. Van Oorschot*

Luby-Rackoff Ciphers: Why XOR Is Not So Exclusive 271
Sarvar Patel, Zulfikar Ramzan, and Ganapathy S. Sundaram

Signatures and Secret Sharing

New Results on Unconditionally Secure Distributed Oblivious Transfer .. 291
*Carlo Blundo, Paolo D'Arco, Alfredo De Santis, and
Douglas R. Stinson*

Efficient Identity Based Signature Schemes Based on Pairings 310
Florian Hess

The Group Diffie-Hellman Problems 325
Emmanuel Bresson, Olivier Chevassut, and David Pointcheval

MAC and Hash Constructions

Secure Block Ciphers Are Not Sufficient for One-Way Hash Functions
in the Preneel-Govaerts-Vandewalle Model 339
Shoichi Hirose

An Efficient MAC for Short Messages 353
Sarvar Patel

RSA and XTR Enhancements

Optimal Extension Fields for XTR	369
<i>Dong-Guk Han, Ki Soon Yoon, Young-Ho Park, Chang Han Kim, and Jongin Lim</i>	
On Some Attacks on Multi-prime RSA	385
<i>M. Jason Hinek, Mo King Low, and Edlyn Teske</i>	
Author Index	405

Selected Areas in Cryptography

9th Annual International Workshop, SAC 2002, St.

John's, Newfoundland, Canada, August 15-16, 2002,

Revised Papers

Nyberg, K.; Heys, H. (Eds.)

2003, XII, 412 p., Softcover

ISBN: 978-3-540-00622-0