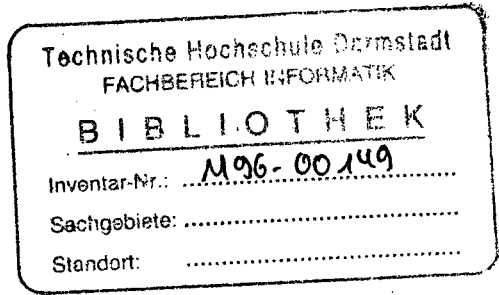


Dieter Gollmann (Ed.)

Fast Software Encryption

Third International Workshop
Cambridge, UK, February 21-23, 1996
Proceedings



Springer

Contents

Block Ciphers – Analysis

Attacks on the HKM/HFX Cryptosystem 1
Xuejia Lai and Rainer A. Rueppel

Truncated Differentials of SAFER 15
Lars R. Knudsen and Thomas A. Berson

On the Weak Keys of Blowfish 27
Serge Vaudenay

Applications

High-Bandwidth Encryption with Low-Bandwidth Smartcards 33
Matt Blaze

ISAAC 41
Robert J. Jenkins Jr.

Hash Functions

A Note on the Hash Function of Tillich and Zémor 51
Willi Geiselmann

Cryptanalysis of MD4 53
Hans Dobbertin

RIPEMD-160: A Strengthened Version of RIPEMD 71
Hans Dobbertin, Antoon Bosselaers, and Bart Preneel

Fast Accumulated Hashing 83
Kaisa Nyberg

Tiger: A Fast New Hash Function 89
Ross Anderson and Eli Biham

Block Ciphers – Proposals

The Cipher SHARK 99
*Vincent Rijmen, Joan Daemen, Bart Preneel, Antoon Bosselaers,
 and Erik De Win*

Two Practical and Provably Secure Block Ciphers: BEAR and LION 113
Ross Anderson and Eli Biham

Unbalanced Feistel Networks and Block Cipher Design 121
Bruce Schneier and John Kelsey

Correlation Analysis

A Comparison of Fast Correlation Attacks 145
Andrew Clark, Jovan Dj. Golić, and Ed Dawson

Correlation Attacks on Stream Ciphers:
 Computing Low-Weight Parity Checks Based on Error-Correcting Codes . 159
Walter T. Penzhorn

On the Security of Nonlinear Filter Generators 173
Jovan Dj. Golić

Block Ciphers – Design Criteria

Faster Luby-Rackoff Ciphers 189
Stefan Lucks

New Structure of Block Ciphers with Provable Security Against
 Differential and Linear Cryptanalysis 205
Mitsuru Matsui

List of Authors 219