Fast Software Encryption Workshop

January 20–22, 1997

Final Program

Monday, January 20, 1997

Session 1: Cryptanalysis I

Chair: Mitsuru Matsui

χ^2 Cryptanalysis of the SEAL Encryption Algorithm, Helena Handschuh, Henri Gilbert

Partitioning Cryptanalysis, C. Harpes, J.L. Massey

The Interpolation Attack on Block Ciphers, Thomas Jakobsen, Lars R. Knudsen

Best Differential Characteristic Search of FEAL, Kazumaro Aoki, Kunio Kobayashi, Shiho Moriai

Session 2: Blockciphers I

Chair: Bart Preneel

New Block Encryption Algorithm MISTY, Mitsuru Matsui

The Design of the ICE Encryption Algorithm, Matthew Kwan

Session 3: Discussion

Chair: Ross Anderson

Discussion Session: Requirements for the Advanced Encryption Standard (AES)

Tuesday, January 21, 1997

Session 4: Stream Ciphers

Chair: Serge Vaudeney

TWOPRIME: A Fast Stream Ciphering Algorithm, Cunsheng Ding, Valtteri Niemi, Ari Renvall, Arto Salomaa

On Nonlinear Filter Generators, Markus Dichtl

Chameleon — A New Kind of Stream Cipher, Ross Anderson, Charalampos Manifavas

Session 5: Cryptanalysis II

Chair: Lars Knudsen

Improving Linear Cryptanalysis of LOKI91 by Probabilistic Counting Method, Kouichi Sakurai, Souichi Furuya

Cryptanalysis of Ladder-DES, Eli Biham

A Family of Trapdoor Ciphers, Vincent Rijmen, Bart Preneel

Session 6: Blockciphers II

Chair: Ronald Rivest

The Block Cipher Square, Joan Daemen, Lars Knudsen, Vincent Rijmen

xmx, a Firmware-Oriented Block Cipher Based on Modular Multiplications, David M'Raihi, David Naccache, Jacques Stern, Serge Vaudenay

Session 7: Recent Results

Chair: Cunsheng Ding

Short contributions on recent results.

Wednesday, January 22, 1997

Session 8: Message Authentication Codes

Chair: Bruce Schneier

MMH: Software Message Authentication in the Gbit/second Rates, Shai Halevi, Hugo Krawczyk

Fast Message Authentication using Efficient Polynomial Evaluation, Valentine Afanassiev, Christian Gehrmann, Ben Smeets

Reinventing the ~~Wheel~~ Travois: Encryption/MAC in 30 ROM Bytes, Gideon Yuval

Session 9: Modes of Operation

Chair: Jacques Stern

All-Or-Nothing Encryption and The Package Transform, Ronald L. Rivest

On the Security of Remotely Keyed Encryption, Stefan Lucks

Sliding Encryption: A Cryptographic Tool for Mobile Agents, Adam Young, Moti Yung

Session 10: Fast Software Encryption

Chair: Ross Anderson

Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor, Bruce Schneier, Doug Whiting

A Fast New DES Implementation in Software, Eli Biham

Optimizing a Fast Stream Cipher for VLIW, SIMD, and Superscalar Processors, Craig S.K. Clapp

Session 11: Discussion

Chair: Bart Preneel

Discussion Session: Security of Cryptosystems: From theory to practice

Presentations at the Recent Results Session

On the Construction of Pseudo-Random Permutations: Luby-Rackoff Revisited, Moni Naor, Omer Reingold

Optimal Galois Field Bases which are not Normal, Preda Mihailescu

Speeding Up with Chinese Remaindering can be Dangerous, Marc Joye, Jean-Jacques Quisqater

An Algorithm to Calculate a Precise Differential Probability of DES F-Function, Kazumaro Aoki, Kazuo Ohta, Takashi Hyodo

On the Security of BEAR and LION, and Ladder-DES, Lars Knudsen

The RSA Data Security Secret Key Challenge, Matt Robshaw

Differential Fault Analysis Revisited, Eli Biham, Adi Shamir

The Guy Fawkes Protocol, Ross Anderson, Bruno Cryspo, Jong-Hyeon Lee, Charalampos Manifavas, Roger Needham