Efficient Explicit Formulae for Genus 2 Hyperelliptic Curves over Prime Fields and Their Implementations
Xinxin Fan and Guang Gong

A fast stream cipher with huge state space and quasigroup filter for software
Makoto Matsumoto, Mutsuo Saito, Takuji Nishimura, and Mariko Hagita

MRHS Equation Systems
Håvard Raddum

Permutation After RC4 Key Scheduling Reveals the Secret Key
Goutam Paul and Subhamoy Maitra

A Generic Method to Design Modes of Operation Beyond the Birthday Bound
David Lefranc, Philippe Painchault, Valérie Rouat, and Emmanuel Mayer

Distinguishing Attack against TPypy
Yukiyasu Tsunoo, Teruo Saito, Takeshi Kawabata, and Hiroki Nakashima

Two Trivial Attacks on Trivium
Alexander Maximov and Alex Biryukov

Linear Cryptanalysis of Non Binary Ciphers with an Application to SAFER
Thomas Baignères, Jacques Stern, and Serge Vaudenay

Collisions for 70-step SHA-1: On the Full Cost of Collision Search
Christophe De Cannière, Florian Mendel, and Christian Rechberger

Revisiting correlation-immunity in filter generators
Aline Gouget and Hervé Sibert

Cryptanalysis of White Box DES Implementations
Louis Goubin, Jean-Michel Masereel, and Michael Quisquater

Analysis of countermeasures against access driven cache attacks on AES
Johannes Blömer and Volker Krummel

Passive-only Key Recovery Attacks on RC4
Serge Vaudenay and Martin Vuagnoux

Attacks on the ESA-PSS-04-151 MAC Scheme
Georg Illies and Marian Margraf

Cryptanalysis of the CRUSH Hash Function
Matt Henricksen and Lars R. Knudsen

Koblitz Curves and Integer Equivalents of Frobenius Expansions
Billy Bob Brumley and Kimmo Järvinen

Reduced Complexity Attacks on the Alternating Step Generator
Shahram Khazaei, Simon Fischer, and Willi Meier

Power Analysis for Secret Recovering and Reverse Engineering of Public Key Algorithms
Frederic Amiel, Benoit Feix, and Karine Villegas

The Delicate Issues of Addition with Respect to XOR Differences
Gaoli Wang, Nathan Keller, and Orr Dunkelman

Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings
Brecht Wyseur, Wil Michiels, Paul Gorissen, and Bart Preneel

Explicit formulas for multiplication in GF(3^(6m))
Elisa Gorla, Christoph Puttmann, and Jamshid Shokrollahi

The Security of the Extended Codebook (XCB) Mode of Operation
David A. McGrew and Scott R. Fluhrer

Extended BDD-based Cryptanalysis of Keystream Generators
Dirk Stegemann

Another Look at Square Roots (and Other Less Common Operations) in Fields of Even Characteristic
Roberto M. Avanzi

Improved Side-Channel Collision Attacks on AES
Andrey Bogdanov