

**Lecture Notes in
Computer Science**

1008

Bart Preneel (Ed.)

Fast Software Encryption

**Second International Workshop
Leuven, Belgium, December 1994
Proceedings**



Springer

Lecture Notes in Computer Science

1008

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Bart Preneel (Ed.)

Fast Software Encryption

Second International Workshop
Leuven, Belgium, December 14-16, 1994
Proceedings



Springer

Series Editors

Gerhard Goos
Universität Karlsruhe
Vincenz-Priessnitz-Straße 3, D-76128 Karlsruhe, Germany

Juris Hartmanis
Department of Computer Science, Cornell University
4130 Upson Hall, Ithaca, NY 14853, USA

Jan van Leeuwen
Department of Computer Science, Utrecht University
Padualaan 14, 3584 CH Utrecht, The Netherlands

Volume Editor JAN 16 1995

Bart Preneel
Department Elektrotechniek-ESAT, Katholieke Universiteit Leuven
Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Fast software encryption : second international workshop,
Leuven, Belgium, December 14 - 16, 1994 ; proceedings / Bart
Preneel (ed.) - Berlin ; Heidelberg ; New York ; Barcelona ;
Budapest ; Hong Kong ; London ; Milan ; Paris ; Tokyo :
Springer, 1995

(Lecture notes in computer science ; Vol. 1008)

ISBN 3-540-60590-8

NE: Preneel, Bart [Hrsg.]; GT

CR Subject Classification (1991): E.3, F2.1, E.4, G.2.1, G.4

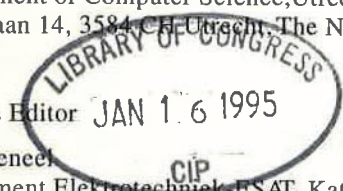
ISBN 3-540-60590-8 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1995
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10487173 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

QA76
.9
.A25 F37
1995
copy 1



6000
95-45832

CONTENTS

<i>Introduction</i>	1
Bart Preneel	

Session 1: Stream Ciphers—Design

Chair: Dieter Gollmann

<i>Clock-controlled pseudorandom generators on finite groups</i>	6
Ulrich Baum and Simon Blackburn	
<i>On random mappings and random permutations</i>	22
William G. Chambers	
<i>Binary cyclotomic generators</i>	29
Cunsheng Ding	
<i>Construction of bent functions and balanced Boolean functions with high nonlinearity</i>	61
Hans Dobbertin	
<i>Additive and linear structures of cryptographic functions</i>	75
Xuejia Lai	

Session 2: Block Ciphers—Design

Chair: James Massey

<i>The RC5 encryption algorithm</i>	86
Ronald L. Rivest	
<i>The MacGuffin block cipher algorithm</i>	97
Matthew Blaze and Bruce Schneier	
<i>S-boxes and round functions with controllable linearity and differential uniformity</i>	111
Kaisa Nyberg	
<i>Properties of linear approximation tables</i>	131
Luke O'Connor	

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.