

1. Record Nr.	UNINA9910483643003321
Titolo	Selected Areas in Cryptography : 14th International Workshop, SAC 2007, Ottawa, Canada, August 16-17, 2007, Revised Selected Papers / / edited by Carlisle Adams, Ali Miri, Michael Wiener
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-77360-6
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (X, 412 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4876
Disciplina	001.5436
Soggetti	Cryptography Data encryption (Computer science) Data protection Electronic data processing - Management Algorithms Computer networks Application software Cryptology Data and Information Security IT Operations Computer Communication Networks Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Reduced Complexity Attacks on the Alternating Step Generator -- Extended BDD-Based Cryptanalysis of Keystream Generators -- Two Trivial Attacks on Trivium -- Collisions for 70-Step SHA-1: On the Full Cost of Collision Search -- Cryptanalysis of the CRUSH Hash Function -- Improved Side-Channel Collision Attacks on AES -- Analysis of Countermeasures Against Access Driven Cache Attacks on AES -- Power Analysis for Secret Recovering and Reverse Engineering of Public Key Algorithms -- Koblitz Curves and Integer Equivalents of Frobenius Expansions -- Another Look at Square Roots (and Other Less Common

Operations) in Fields of Even Characteristic -- Efficient Explicit Formulae for Genus 2 Hyperelliptic Curves over Prime Fields and Their Implementations -- Explicit Formulas for Efficient Multiplication in -- Linear Cryptanalysis of Non Binary Ciphers -- The Delicate Issues of Addition with Respect to XOR Differences -- MRHS Equation Systems -- A Fast Stream Cipher with Huge State Space and Quasigroup Filter for Software -- Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings -- Cryptanalysis of White Box DES Implementations -- Attacks on the ESA-PSS-04-151 MAC Scheme -- The Security of the Extended Codebook (XCB) Mode of Operation -- A Generic Method to Design Modes of Operation Beyond the Birthday Bound -- Passive-Only Key Recovery Attacks on RC4 -- Permutation After RC4 Key Scheduling Reveals the Secret Key -- Revisiting Correlation-Immunity in Filter Generators -- Distinguishing Attack Against TPpy.

---

## Sommario/riassunto

SAC 2007 was the 14th in a series of annual workshops on Selected Areas in Cryptography. This is the first time this workshop was held at the University of Ottawa. Previous workshops were held at Queen's University in Kingston (1994, 1996, 1998, 1999, and 2005), Carleton University in Ottawa (1995, 1997, and 2003), University of Waterloo (2000 and 2004), Fields Institute in Toronto (2001), Memorial University of Newfoundland in St. Johns (2002), and Concordia University in Montreal (2006). The intent of the workshop is to provide a stimulating atmosphere where researchers in cryptology can present and discuss new work on selected areas of current interest. The themes for SAC 2007 were: – Design and analysis of symmetric key cryptosystems – Primitives for symmetric key cryptography, including block and stream ciphers, hash functions, and MAC algorithms – Efficient implementations of symmetric and public key algorithms – Innovative cryptographic defenses against malicious software A total of 73 papers were submitted to SAC 2007. Of these, one was withdrawn by the authors, and 25 were accepted by the Program Committee for presentation at the workshop. In addition to these presentations, we were fortunate to have two invited speakers: – Dan Bernstein: “Edwards Coordinates for Elliptic Curves” – MotiYung: “Cryptography and Virology Inter-Relationships.” This talk was designated the Stanford Tavares Lecture. We are grateful to the Program Committee and the many external reviewers for their hard work and expertise in selecting the program.

---