

1. Record Nr.	UNINA9910151936303321
Autore	Daskalopoulos Panagiota
Titolo	Degenerate Diffusions [[electronic resource] ] : Initial Value Problems and Local Regularity Theory // Panagiota Daskalopoulos, Carlos E. Kenig
Pubbl/distr/stampa	Zuerich, Switzerland, : European Mathematical Society Publishing House, 2007
ISBN	3-03719-533-9
Descrizione fisica	1 online resource (207 pages)
Collana	EMS Tracts in Mathematics (ETM) ; 1
Classificazione	35-xx
Soggetti	Differential equations Partial differential equations
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	<p>The book deals with existence, uniqueness, regularity and asymptotic behavior of solutions to the initial value problem (Cauchy problem) and the initial-Dirichlet problem for a class of degenerate diffusions modeled on the porous medium type equation <math>u_t = u^m</math>, <math>m &gt; 0</math>, <math>u &gt; 0</math>. Such models arise in plasma physics, diffusions through porous media, thin liquid film dynamics as well as in geometric flows such as the Ricci flow on surfaces and the Yamabe flow. The approach presented to these problems is through the use of local regularity estimates and Harnack type inequalities, which yield compactness for families of solutions. The theory is quite complete in the slow diffusion case (<math>m &gt; 1</math>) and in the supercritical fast diffusion case (<math>m_c &lt; m &lt; 1</math>, <math>m_c = (n - 2) / (n - 1)</math>) while many problems remain in the range <math>m &lt; m_c</math>. All of these aspects of the theory are discussed in the book. The book is addressed to both researchers and to graduate students with a good background in analysis and some previous exposure to partial differential equations.</p>

2. Record Nr.	UNINA9910484329303321
Titolo	Selected Areas in Cryptography : 16th International Workshop, SAC 2009, Calgary, Alberta, Canada, August 13-14, 2009, Revised Selected Papers // edited by Michael J. Jacobson, Vincent Rijmen, Rei Safavi-Naini
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-05445-5
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIII, 467 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5867
Classificazione	DAT 465f SS 4800
Altri autori (Persone)	JacobsonMichael J RijmenVincent <1970-> Safavi-NainiReihanah
Disciplina	004n/a
Soggetti	Cryptography Data encryption (Computer science) Computer programming Data protection Data structures (Computer science) Information theory Coding theory Computer science - Mathematics Discrete mathematics Cryptology Programming Techniques Data and Information Security Data Structures and Information Theory Coding and Information Theory Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Hash Functions I -- Practical Collisions for SHAMATA-256 -- Improved

Cryptanalysis of the Reduced Grøstl Compression Function, ECHO Permutation and AES Block Cipher -- Cryptanalyses of Narrow-Pipe Mode of Operation in AURORA-512 Hash Function -- Miscellaneous Techniques -- More on Key Wrapping -- Information Theoretically Secure Multi Party Set Intersection Re-visited -- Real Traceable Signatures -- Hash Functions II -- Cryptanalysis of Hash Functions with Structures -- Cryptanalysis of the LANE Hash Function -- Practical Pseudo-collisions for Hash Functions ARIRANG-224/384 -- Hardware Implementation and Cryptanalysis -- A More Compact AES -- Optimization Strategies for Hardware-Based Cofactorization -- More on the Security of Linear RFID Authentication Protocols -- Differential Fault Analysis of Rabbit -- An Improved Recovery Algorithm for Decayed AES Key Schedule Images -- Block Ciphers -- Cryptanalysis of the Full MMB Block Cipher -- Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis -- Improved Integral Attacks on MISTY1 -- New Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia-128 -- Modes of Operation -- Format-Preserving Encryption -- BTM: A Single-Key, Inverse-Cipher-Free Mode for Deterministic Authenticated Encryption -- Implementation of Public Key Cryptography -- On Repeated Squarings in Binary Fields -- Highly Regular m-Ary Powering Ladders -- An Efficient Residue Group Multiplication for the  $\mathbb{F}_T$  Pairing over  $\mathbb{F}_T$  -- Compact McEliece Keys from Goppa Codes -- Hash Functions and Stream Ciphers -- Herding, Second Preimage and Trojan Message Attacks beyond Merkle-Damgård -- Cryptanalysis of Dynamic SHA(2) -- A New Approach for FCSRs -- New Cryptanalysis of Irregularly Decimated Stream Ciphers.

---

Sommario/riassunto

This volume constitutes the selected papers of the 16th Annual International Workshop on Selected Areas in Cryptography, SAC 2009, held in Calgary, Alberta, Canada, in August 13-14 2009. From a total of 99 technical papers, 27 papers were accepted for presentation at the workshop. They cover the following topics: hash functions, on block and stream ciphers, public key schemes, implementation, and privacy-enhancing cryptographic systems.

---