1. Record Nr.	UNINA9910485140003321
Titolo	Selected Areas in Cryptography : 15th Annual International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, 2008 / / edited by Roberto Avanzi, Liam Keliher, Francesco Sica
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-04159-0
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XI, 457 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5381
Altri autori (Persone)	AvanziRoberto KeliherLiam SicaFrancesco
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Data protection Coding theory Information theory Data structures (Computer science) Computer science - Mathematics Discrete mathematics Cryptology Data and Information Security Coding and Information Theory Data Structures and Information Theory Discrete Mathematics in Computer Science Symbolic and Algebraic Manipulation
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	Elliptic and Hyperelliptic Curve Arithmetic -- Faster Halvings in Genus 2 -- Efficient Pairing Computation on Genus 2 Curves in Projective Coordinates -- On Software Parallel Implementation of Cryptographic Pairings -- Block Ciphers I -- The Cryptanalysis of Reduced-Round SMS4 -- Building Secure Block Ciphers on Generic Attacks Assumptions

Sommario/riassunto

The book in front of you contains the proceedings of SAC 2008, the 15th - nual Workshop on Selected Areas in Cryptography. SAC 2008 took place during August 14-15 at Mount Allison University, Sackville, New Brunswick, Canada. This was the ?rst time that SAC was hosted in New Brunswick, and the second time in an Atlantic Canadian province. Previous SAC workshops were held at Queen's University in Kingston (1994, 1996, 1998, 1999, and 2005), at Carleton University in Ottawa (1995, 1997, 2003), at the University of Waterloo (2000, 2004), at the Fields Institute in Toronto (2001), at Memorial University of Nfoundland at St. John's (2002), at Concordia University in Montreal (2006) and at the University of Ottawa (2007). The intent ofthe workshopseriesis to provide a relaxedatmospherein which researchers in cryptography can present and discuss new work on selected areas of current interest. The SAC workshop series has ?rmly established itself as an international forum for intellectual exchange in cryptological research. Theresponsibilityforchoosingthe venueofeachSACworkshopandappoi- ingtheCo-chairslieswiththeSACOrganizingBoard.TheCo-chairsthenchoose the Program Committee in consultation with the Board. Hence, we would like to expressour gratitudeto the SAC OrganizingBoardfor giving usthe mandate to organize SAC 2008, and for their invaluable feedback while assembling the Program Committee.