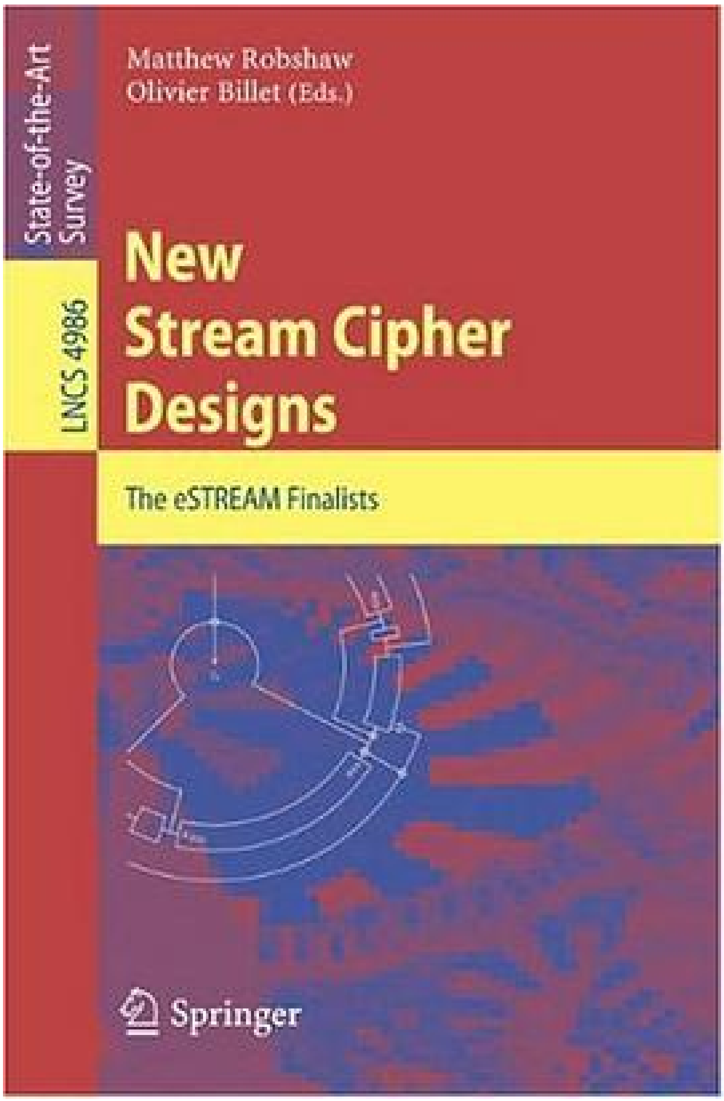
New Stream Cipher Designs



New Stream Cipher Designs_下载链接1_

著者:Billet, Olivier 编

出版者:Springer

出版时间:2008-08-27

装帧:Paperback

isbn:9783540683506

This state-of-the-art survey presents the outcome of the eSTREAM Project, which was launched in 2004 as part of ECRYPT, the European Network of Excellence in Cryptology (EU Framework VI). The goal of eSTREAM was to promote the design of new stream ciphers with a particular emphasis on algorithms that would be either very fast in software or very resource-efficient in hardware. Algorithm designers were invited to submit new stream cipher proposals to eSTREAM, and 34 candidates were proposed from around the world. Over the following years the submissions were assessed with regard to both security and practicality by the cryptographic community, and the results were presented at major conferences and specialized workshops dedicated to the state of the art of stream ciphers. This volume describes the most successful of the submitted designs and, over 16 chapters, provides full specifications of the ciphers that reached the final phase of the eSTREAM project. The book is rounded off by two implementation surveys covering both the software- and the hardware-oriented finalists.

作者介绍:

目录:

New Stream Cipher Designs_下载链接1_

标签

评论

New Stream Cipher Designs_下载链接1_

书评

New Stream Cipher Designs_下载链接1_