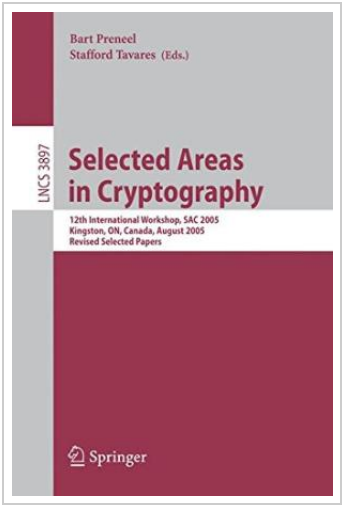

Selected Areas in Cryptography

By Preneel, Bart / Tavares, Stafford

Condition: New. Publisher/Verlag: Springer, Berlin | 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers | This book constitutes the thoroughly refereed post-proceedings of the 12th International Workshop on Selected Areas in Cryptography, SAC 2005, held in Canada in August 2005. The 25 revised full papers presented were carefully reviewed and selected from 96 submissions for inclusion in the book. The papers are organized in topical sections. | Stream Ciphers I.- Conditional Estimators: An Effective Attack on A5/1.- Cryptanalysis of the F-FCSR Stream Cipher Family.- Fault Attacks on Combiners with Memory.- Block Ciphers.- New Observation on Camellia.- Proving the Security of AES Substitution-Permutation Network.- Modes of Operation.- An Attack on CFB Mode Encryption as Used by OpenPGP.- Parallelizable Authentication Trees.- Improved Time-Memory Trade-Offs with Multiple Data.- Public Key Cryptography.- A Space Efficient Backdoor in RSA and Its Applications.- An Efficient Public Key Cryptosystem with a Privacy Enhanced Double Decryption Mechanism.- Stream Ciphers II.- On the (Im)Possibility of Practical and Secure Nonlinear Filters and Combiners.- Rekeying Issues in the MUGI Stream Cipher.- Key Establishment Protocols and Access Control.- Tree-Based Key Distribution Patterns.- Provably Secure Tripartite Password Protected Key Exchange Protocol Based on Elliptic Curves.- An Access...

Reviews

If you need to adding benefit, a must buy book. It is actually rally interesting throgh reading time period. It is extremely difficult to leave it before concluding, once you begin to read the book.

-- ***Olen Mills***

An extremely awesome ebook with perfect and lucid reasons. This is certainly for all who statte there was not a well worth looking at. Your daily life span will likely be convert as soon as you complete looking over this book.

-- ***Anahi Heaney***