1. Record Nr. UNISA996203598503316

| | |
|---|---|
| Titolo | Progress in Cryptology – AFRICACRYPT 2014 [[electronic resource] ] : 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings / / edited by David Pointcheval, Damien Vergnaud |
| Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014 |
| ISBN | 3-319-06734-6 |
| Edizione | [1st ed. 2014.] |
| Descrizione fisica | 1 online resource (XIV, 476 p. 92 illus.) : online resource |
| Collana | Security and Cryptology ; ; 8469 |
| Disciplina | 005.82 |
| Soggetti | Computer security<br>Data encryption (Computer science)<br>Coding theory<br>Information theory<br>Numerical analysis<br>Computers<br>Management information systems<br>Computer science<br>Systems and Data Security<br>Cryptology<br>Coding and Information Theory<br>Numeric Computing<br>Computation by Abstract Devices<br>Management of Computing and Information Systems |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Bibliographic Level Mode of Issuance: Monograph |
| Nota di contenuto | New Results for Rank-Based Cryptography -- Public-Key Cryptography -- Proxy Re-Encryption Scheme Supporting a Selection of Delegatees -- Trapdoor Privacy in Asymmetric Searchable Encryption Schemes -- Kurosawa-Desmedt Key Encapsulation Mechanism, Revisited -- Hash Functions -- Differential Biases in Reduced-Round Keccak -- Practical Distinguishers against 6-Round Keccak-f Exploiting Self-Symmetry -- |

Preimage Attacks on Reduced-Round Stribog -- Secret-Key Cryptanalysis -- Breaking the IOC Authenticated Encryption Mode -- New Treatment of the BSW Sampling and Its Applications to Stream Ciphers -- Multidimensional Zero-Correlation Linear Cryptanalysis of E2 -- Public-Key Cryptanalysis and Number Theory Further Improvement of Factoring RSA Moduli with Implicit Hint -- New Attacks on the RSA Cryptosystem -- Formulae for Computation of Tate Pairing on Hyperelliptic Curve Using Hyperelliptic Nets -- Hardware Implementation -- New Speed Records for Montgomery Modular Multiplication on 8-bit AVR Microcontrollers -- Minimizing S-Boxes in Hardware by Utilizing Linear Transformations -- Efficient Masked S-Boxes Processing – A Step Forward -- A More Efficient AES Threshold Implementation -- Protocols -- Constant Rounds Almost Linear Complexity Multi-party Computation for Prefix Sum -- Position-Based Cryptography from Noisy Channels -- Lattice-Based Cryptography -- A Comparison of the Homomorphic Encryption Schemes FV and YASHE -- Towards Lattice Based Aggregate Signatures -- Public-Key Cryptography -- A Second Look at Fischlin's Transformation -- Anonymous IBE from Quadratic Residuosity with Improved Performance -- Expressive Attribute Based Signcryption with Constant-Size Ciphertext -- Secret-Key Cryptography.-DRECON: DPA Resistant Encryption by Construction -- Counter-bDM: A Provably Secure Family of Multi-Block-Length Compression Functions -- Universal Hash-Function Families: From Hashing to Authentication.

Sommario/riassunto

This book constitutes the refereed proceedings of the 7th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICACRYPT 2014, held in Marrakesh, Morocco in May 2014. The 26 papers presented  together with 1 invited talk were carefully reviewed and selected from 83 submissions. The aim of Africacrypt 2014 is to provide an international forum for practitioners and researchers from industry, academia and government from all over the world for a wide ranging discussion of all forms of cryptography and its applications as follows: Public-Key Cryptography, Hash Functions, Secret-Key Cryptanalysis, Number Theory, Hardware Implementation, Protocols, and Lattice-based Cryptography.