<<Topics in Cryptology>>

<<Topics in Cryptology - CT-RSA 2001: The Cryptographer's Track at RSA Conference 2001 San Francisco, CA, USA, April 8-12, 2001 Proceedings (   )>>

13   ISBN   9783540418986

10   ISBN   3540418989

        2001-12

        1 edition (2001   5   1   )

   David Naccache

   470

                            PDF

             http://www.tushu007.com

<<Topics in Cryptology>>

This book constitutes the refereed proceedings of the Cryptographers' Track at RSA Conference 2001, CT-RSA 2001, in San Francisco, CA, USA in April 2001.The 33 revised full papers presented were carefully reviewed and selected from 65 submissions. The papers are organized in topical sections on new cryptosystems; RSA; symmetric cryptography; gambling and lotteries; reductions, constructions, and security proofs; flaws and attacks; implementation; multivariate cryptography; number theoretic problems; passwords and credentials; and protocols.

<<Topics in Cryptology>>

New Cryptosystems Faster Generation of NICE-Schnorr-Type Signatures   New Key Agreement Protocols in Braid Group CryptographyRSA   Improving SSL Handshake Performance via Batching   From Fixed-Length Messages to Arbitrary-Length Messages Practical RSA   Signature Padding Schemes   An Advantage of Low-Exponent RSA with Modulus Primes Sharing Least   Significant BitsSymmetric Cryptography   On the Strength of Simply-Iterated Feistel Ciphers with Whitening Keys   Analysis of SHA-1 in Encryption Mode   Fast Implementation and Fair Comparison of the Final Candidates for   Advanced Encryption Standard Using Field Programmable Gate Arrays Gambling and Lotteries   Fair e-Lotteries and e-Casinos   Secure Mobile GamblingReductions, Constructions and Security Proofs   Formal Security Proofs for a Signature Scheme with Partial Message   Recovery   The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES   REACT: Rapid Enhanced-Security Asymmetric Cryptosystem TransformFlaws and Attacks   Security Weaknesses in Bluetooth   Distinguishing Exponent Digits by Observing Modular Subtractions   On the Power of Misbehaving Adversaries and Security Analysis of the   Original EPOC Implementation   Modular Exponentiation on Fine-Grained FPGA……Multivariate CryptographyNumber Theoretic ProblemsProtocols IProtocols IAuthor Index

<<Topics in Cryptology>>

PDF

:http://www.tushu007.com