1.

Record Nr.	UNISA996465824603316
Autore	Goldwasser Shafi
Titolo	Advances in Cryptology - CRYPTO '88 : Proceedings
Pubbl/distr/stampa	New York, NY : , : Springer, , 2008 ©1990
Descrizione fisica	1 online resource (588 pages)
Collana	Lecture Notes in Computer Science ; ; v.403
Altri autori (Persone)	GoldwasserShafi
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Lecture Notes in Computer Science -- Foreword -- CRYPT0 '88 -- Table of Contents -- Weakening Security Assumptions and Oblivious Transfer -- Introduction -- Definitions -- Standard forms of oblivious transfer -- Nonstandard transfer mechanism -- Making honest reductions more robust -- The general scenario -- The power of noise -- A philosophical remark -- An outline of our reduction -- Acknowledgments -- Refernces -- Limits on the Provable Consequences of One-way Permutations -- Introduction -- Notation and deflnitions -- Uniform Generation -- Polynomial-time relations -- What is uniform generation? -- P = NP and uniform generation -- An application to cryptography -- Random Oracles -- Random function oracles -- Random oracles and uniform generation -- Random Permutation Oracles -- Cryptographic Lower Bounds -- Introduction -- A normal form for secret-key agreement -- Notation and definitions -- Eve's sample space -- Eve's algorithm -- Intersection queries and the secret -- The efficacy of Eve's algorithm -- Related Work and Open Problems -- Acknowledgements -- References -- Generalized Secret Sharing and Monotone Functions -- Introduction -- Preliminaries -- Generalized Secret Sharing -- Generalized Secret Sharing Homomorphisms -- Conclusions -- Acknowledgements -- References -- Everything Provable is Provable in Zero-Knowledge -- Abstract -- Introduction -- Overview of the construction -- Preliminaxies -- Interactive proof systems -- Arthur-Merlin protocols -- Zero-knowledge -- Preliminary results -- Zero-knowledge proofs for all of

NP -- Proof of the main theorem -- Notarized Envelopes: Description and Implement ation -- Introduction to notarized envelopes- -- An implementation of notarized envelopes -- IP in perfect zero-knowledge with envelopes -- References.

A Perfect Zero-Knowledge Proof for a Problem Equivalent to Discrete Logarithm -- ABSTRACT -- INTRODUCTION -- Known Results -- Our Results -- PRELIMINARIES -- Promise Problems and Interactive Proofs -- Perfect Zero-Knowledge Proofs for Promise Problems -- The Discrete Logarithm Problem and a Related Promise Problem -- Notations -- THE PROTOCOL FOR DLPl IN Zp' -- Protocol 1 - Perfect Zero Knowledge Proof with respect to the Honest Verifier -- Protocol 2 - Perfect Zero Knowledge Proof with respect to Any Verifier -- EXTENSIONS -- Generalization of the Protocol to other Cyclic Groups -- Generalization of the Results to Acyclic Groups -- REFERENCES -- Zero-Knowledge With Finite State Verifiers -- Abstract. -- Introduction -- Definitions -- An Example -- Zero Knowledge Interactive Proof Systems -- Old and New Definitions -- Languages Having No Zero Knowledge IPS -- A Language With a Recognition Zero Knowledge IPS -- Related Work -- References -- Intractable Problems in Number Theory -- Abstract. -- Introduction -- Problems related to factoring -- Problems related to discrete logarithms -- Algorithms -- Practical considerations -- Acknowledgements -- References -- A Family of Jacobians Suitable for Discrete Log Cryptosystems -- Abstract. -- Theorem. -- Remarks. -- References -- Computation of Approximate L-th Roots Modulo n and Application to Cryptography -- ABSTRACT -- THE PROBLEMS -- HOW PROBLEMS AROSE -- Problem (1) and its variants -- Problems (2a) and (2b) -- THE ALGORITHMS -- Finding roots with small residual -- Without conditions for x -- With conditions for x -- A Euclidean digression -- Come back to our problems -- 2. Finding something about exact mots -- Inferring some partial information about location of % -- Finding x,, with some help -- CONCLUSION -- ACKNOWLEDGEAMENTS -- REFERENCES -- On the McEliece Public-Key Cryptosystem -- Abstract.

Introduction -- McEliece's Cryptosystem -- Cryptanalysis of the McEliece Cryptosystem -- Factoring the encryption matix -- Recover message from cryptogram and encryption ma- trix -- Main Idea -- One Bit Swapping Attack -- Number of Swaps -- Work factor -- F'urther Improvements -- Search for one correctable error -- Partial search for two correctable errors -- General Attack -- Reduced Public-Key -- Acknowledgement -- References -- A Constraint Satisfaction Algorithm for the Automated Decryption of Simple Substitution Ciphers -- Abstract -- Introduction -- The Database -- The Search Technique -- Interactive Mode -- Extensions -- Performance -- Acknowledgement -- References -- On the Existence of Pseudorandom Generators -- INTRODUCTION -- Previous Results -- Our Results -- Subsequent Results -- MAINRESULT -- Preliminaries -- Levin's Criterion: A Modified Version -- Main Ideas -- The Construction of f' -- The game -- Proof of Theorem 2 -- Extensions -- Further Remarks: -- APPLICATIONS : Pseudorandom Generators Based on Particular Intractabil- ity Assumptions -- PRG Based on the Intractability of the General Factoring Problem -- PRG Based on the Intractability of Decoding Random Linear Codes -- PRG Based on the Average Difficulty of Cornbinatorial Problems -- ACKNOWLEDGEMENTS -- REFERENCES -- ON THE RANDOMNESS OF LEGENDRE AND JACOBI SEQUENCES -- Introduction -- Notation -- Known Results On the Distribution of Squares Jlodulo a Prime -- Jacobi Sequences are Harder to Predict than Legendre Sequences -- Emphirical Tests -- Practical Implementation -- Generalizations -- The Linear Congruence hlethod -- Using Other

Sommario/riassunto

The papers in this voluriic were presented at the CHYP'I'O 'SS conf-
ence on theory and applications of cryptography, Iicld August 21-2, j.
19SS in Sarita Uarbara, ('alifornia. The conference was sponsored hy the
Int- national AssociatioIi for C'ryptologic Research (IAC'R) and hosted
by the computer science depart incnt at the IIniversity of California at
Sarita D- ha ra . 'rile 4-1 papers presented hcrc coniprise: 35 papers
selected from 61 - tcwded abstracts subniittctl in response to the call
for papcrs, 1 invitcd prv sentations, and 6 papers sclccted from a large
niiiii1, cr of informal UIIIJ) sewion present at ionc. The papers wcrc
chosen by the program committee on the lja\is of tlic perceived
originality, quality and relevance to the field of cryptography of the
cxtcndcd allst ract5 suhriiitted. 'I'hc su1, missioris wv riot otlierwise rc.
fcrcc(l. a id ofteri rcprescnt prcliininary reports on continuing rcscarc.
11. It is a pleasure to tharik many colleagues. Ilarold Iredrickscri sing-
made CRJ'PTO '88 a successful realit, y. Eric Dacli, Pad Ijnrret. haridedly
Tom Bersori, Gilles Brassard, Ocled Goldreich, Andrew Odlyzko.
C'liarles Rackoff arid Ron Rivest did excellerit work on the program
comrriittcc in piittirig the technical program together, assisted by kind
outsick reviekvers.