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

Character Values -- Conclusion and Open Problems -- References -- EFFICIENT, PERFECT RANDOM NUMBER GENERATORS -- Abstract -- The Complexity Assumption for the Polynomial Random Generator -- Hypothesis 2.1 -- Fact 2.2 -- Theorem 2.3 -- Corollary 2.4. Corollary 2.5 -- Theorem 2.6 -- Thearem 2.7 -- 3. The Sequential and the Parallel Polynomial Generator -- Theorem 3.1 -- Theorem 3.2 -- Corollary 3.3 -- Theorem 3.4 -- Theorem 3.5 -- 4. Open Problems: Random Number Generators Based on 1 Prime Modulus -- Problem 4.1. -- Problem 4.2. -- Corollary 4.3 -- How To Sign Given Any Trapdoor Function -- Abstract -- INTRODUCTION -- SIGNATURE SCHEMES AND THEIR SECU- RITY -- Components of a Signature Scheme -- Security against Adaptive Chosen Message Attacks -- TRAPDOOR PERMUTATIONS -- AN OVERVIEW OF THE SCHEME -- Background -- Untitled -- The Signature Scheme -- Why is this Secure? -- THE SCHEME AND PROOF OF SECURITY -- Preliminary Notation and Definitions -- Building Blocks for Signing -- Generating Keys -- What is a Signature? -- The Signing Algorithm and Signature Corpus -- The Verification Algorithm -- Extracting Information From a Forgery -- Proof of Security -- VARIATIONS AND IMPROVEMENTS -- References -- A "Paradoxical" Indentity-Based Signature Scheme Resulting from Zero-Knowledge -- ABSTRACT -- Introduction -- The GQ authentication scheme -- Security of the GQ scheme -- Protocols of cooperation between entities -- Entities with same exponent and different identities -- Two entities with the same identity and different expo- nents -- Interactively authenticating both cards and -- Swapping to signatures by removing interactiv- ity -- The identity-based signature scheme -- Exchange authentication: a priori versus a pos- teriori? -- References -- A Modification of the Fiat-Shamir Scheme -- Abstract -- Introduction -- Some Number-Theoretic Results -- Sequential Version -- Parallel Version -- Applications -- Efficiency -- Conclusion -- Acknowledgements -- References -- An Improvement of the Fiat-Shamir Identification and Signature Scheme -- Abstract -- Introduction. -- The original Fiat-Shamir Scheme. The New Improvement -- Remark -- A Basic Theory of Public and Private Cryptosystems -- References -- Proving Security Against Chosen Ciphertext Attacks -- Abstract -- Introduction -- Our Model Versus the Old One -- The Robustness of Our Result -- Applications of our Result -- What's Coming -- Preliminaries -- Notations and Conventions -- Number Theory -- A Complexity Assumption -- Single-Theorem Non-Interactive Zero-Knowledge Proofs -- The Proof System (P,V) -- A Rough Idea of why (P,V) is a Single-Theorem Non- -- Security Against Chosen Ciphertext Attack -- References -- Non-Interactive Zero-Knowledge with Preprocessing -- Abstract -- A quick and dirty exposition of our results -- Introduction -- Preliminaries -- Non-Interactive Zero-Knowledge Proof-Systems -- The model -- Our protocol -- The language V -- The implementation -- Open Problems -- References -- The Noisy Oracle Problem -- Abstract -- Introduction -- TheModel -- Polynomial Time Verifiers -- Knowledge complexity -- Further Research -- References -- On Generating Solved Instances of Computational Problems -- Introduction -- Terminology, Notation, and Conventions -- Invulnerable Generators -- Discussion, Related Work, and Open Problems -- Acknowledgements -- References -- Bounds and Constructions for Authentication - Secrecy Codes with - Splitting -- Secrecy -- Bounds on Pdi and b -- Constructions for authentication codes "with arbi- trary source distribution -- Authentication codes derived from partial geometries -- Authentication codes derived from designs -- References -- Untraceable Electronic Cash t -- Introduction -- Untraceable Coins -- Proving Multiple Spending -- Untraceable

Checks -- Blacklisting Withdrawals -- Further Work -- Acknowledgements -- References -- PAYMENT SYSTEMS AND CREDENTIAL MECHANISMS WITH PROVABLE SECURITY AGAINST ABUSE BY INDIVIDUALS -- Summary -- Related Work.
Basic Results.

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 llniversity 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.