1.

Record Nr.	UNISA996465813803316
Autore	Brassard Gilles
Titolo	Advances in Cryptology - CRYPTO '89 : Proceedings
Pubbl/distr/stampa	New York, NY : , : Springer, , 1995 ©1990
Descrizione fisica	1 online resource (628 pages)
Collana	Lecture Notes in Computer Science ; ; v.435
Altri autori (Persone)	BrassardGilles
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Lecture Notes inComputer Science -- CRYPTO '89 -- Organizers -- Preface -- References -- Contents -- KEYING THE GERMAN NAVY'S ENIGIMA -- Making Conditionally Secure Cryptosystems Unconditionally Abuse-Free in a General Context -- Introduct ion -- Formal model for abuses and abuse-freeness -- A general solution -- A BUILDING BLOCK -- OUR SOLUTION -- Conclusions and open problems -- REFERENCES -- On the Existence of Bit Commitment Schemes and Zero-Knowledge Proofs -- Abstract -- Introduction and Related Work. -- Main Result -- Non MA-protocols -- References -- Problems with the Normal Use of Cryptography for Providing Security on Unclassified Networks -- Introduct ion -- A Password is Not a Key -- Passwords are often shorter than the look -- Re-used Passwords Lead to Dif3culties -- Broadcast of Clear Text LLKeysi"s Poor Practice -- Known Plaintext Attacks are not Foiled by Salt -- Unauthenticated Authentication Servers lead to Problems -- Tampering of Signed Packets is often Possible -- Difficult Factoring Effect the Security of Discrete Logs -- Bad Information Leads to Bad Decisions -- User Errors are Compromise otherwise Good Systems -- Authentication for the Academic World -- Conclusion -- References -- The use of Encryption in Kerberos for Network Authentication -- Introduction -- Terminology -- Kerberos overview -- Version 4 Protocol -- Encryption -- Cryptographic checksums -- Cryptanalysis -- Application protocols -- Authentication Service -- Client to Server -- Ticket-Granting Service -- Integrity-protected messages -- Privacy-

protected messages -- Planned version 5 changes -- Conclusion -- Acknowledgments -- References -- UNIX Password Security - Ten Years Later* -- Introduction -- Fast Crypt Implementations -- Precomputed Encrypted Dictionaries -- Improving Password Security -- Known Encryption Algorithm.

Acceptable Running Times -- Encrypted Password Availability -- Decreasing Password Guessability -- Other Approaches -- Conclusion -- References -- A High-speed Crypt Implementation -- Overview of Crypt -- The Speed-Crypt Implementation -- Algorithm Modifkations -- Subkey Generation -- Table Lookup -- Data Representation -- Salting -- System Issues -- Implementation Alternatives -- Speed Measurements -- Conclusion -- Practical Problems with a Cryptographic Protection Scheme -- Introduction -- History -- Architecture -- Local Actions -- Remote Actions -- Security Problems -- A Server-based solution -- Encryption Server -- Problems -- Re-design, no server -- Conclusions -- Notes -- References -- THE SMART DISKETTE -- Security and Personal Computers -- A Token-based Solution -- The Smart Diskette Solution -- Implementing the Smart Diskette -- Conclusions -- References -- On the Quadratic Spans of Periodic Sequences1 -- Introduction -- Definitions and Main Results -- LIST OF REFERENCES -- The Shortest Feedback Shift Register That Can Generate A Given Sequence -- Introduction -- Theor -- Maximum Order Complexity -- The Maximum Order Complexity Profile -- The Typical Complexity Profile -- Sequence Analysis and FSR Synthesis -- Conclusions -- References -- Perfect Local Randomness in Pseudo-random Sequences -- Introduction -- Generators Achieving Perfect Local Randomness -- Locally-Randomized Pseudo-random Number Generators -- Extensions of the Concept of Local Randomization -- Applications and Conclusions -- Acknowledgement -- References -- Sparse Pseudorandom Distributions -- INTRODUCTION -- DEFINITIONS -- THE EXISTENCE OF SPARSE PSEUDORANDOM ENSEMBLES -- THE COMPLEXITY OF APPROXIMATING PSEUDORANDOM ENSEMBLES -- POLYNOMIAL-TIME EVASIVE PSEUDORANDOM ENSEMBLES -- ON THE SEQUENTIAL COMPOSITION OF ZERO-KNOWLEDGE PROTOCOLS -- ACKNOWLEDGEMENTS -- REFERENCES.

Bit Commitment Using Pseudo-Randomness* -- Introduction -- Definitions -- The Bit Commitment -- Efficient Commit to Many Bits -- Conclusions -- References -- How to Predict Congruential Generators -- INTRODUCTION -- DEFINITIONS AND NOTATION -- THE PREDICTING ALGORITHM -- First Stage -- Second Stage -- VECTOR-VALUED RECURRENCES -- CONCLUDING REMARKS -- ACKNOWLEDGEMENTS -- REFERENCES -- A Chosen Text Attack on The Modified Cryptographic Checksum Algorithm of Cohen and Huang -- INTRODUCTION -- THE SCHEME OF COHEN AND HUANG -- WEAKNESS OF THE MODULO REDUCTION -- DEFUVING THE FIRST s BITS OF THE KEY K -- Deriving the most significant bit of K -- Deriving the B most significant bits of K -- Further extensions -- SUMMARY -- References -- On the Linear Consistency Test (LCT) in Cryptanalysis with Applications * -- Introduction -- References -- Batch RSA -- Abstract -- Introduction -- Background and Central Observation -- BatchRSA -- Notes on Security -- Constants and Practical Considerations -- Acknowledgements -- References -- On the Implementation of Elliptic Curve Cryptosystems -- Abstract -- Introduction -- Some basic definitions -- The order of the group -- A Cryptographically Useful Subclass of Elliptic Curves -- Choice of the Elliptic Curve and Cyclic Subgroup -- Numerical Results -- Acknowledgement -- Bibliography -- New Paradigms for Digit al Signatures and Message AuthenticationBased on Non-Interactive Zero

Knowledge Proofs -- Introduction -- A NIZK Proof Based Paradigm -- Non-Interactive Zero Knowledge Proof Systems -- Publicly Verifiable NIZK Proof Systems -- Random Functions -- Related Results -- Notation -- Non-Interactive Zero Knowledge Proof Systems -- Definition -- Remarks -- A Look at Available Implementations -- NIZK Proofs and Digital Signatures -- How to Sign -- Comparison with Previous Signature Schemes -- Assumptions -- Security.

Further Applications of the NIZK Paradigm -- Message Authentication between Pairs of Users -- Memoryless Distribution of Identification Numbers -- NIZK Proof Systems with Public Verifiability -- A Simple Scheme -- Zero Knowledge to Many Users Simultaneously -- History Independent Signatures -- Appendix: Proof of Security for the Signature Scheme -- Appendix: Using a Simpler Zero KnowledgeDefinition -- References -- Undeniable Signatures -- INTRODUCTION & MOTIVATION -- CRYPTOGRAPHSIECT TING -- PROTOC -- UNDENIABILIT -- UNFORGEABIL -- BLINDIN -- CONCLUSI -- ACKNOWLEDGEME -- REFERENCE -- A CERTIFIED DIGITAL SIGNATURE -- Introduction -- One Way Functions -- The Lamport-Diffie One Time Signature -- An Improved One Time Signature -- The Winternitz Improvement -- Tree Authentication -- The Path Regeneration Algorithm -- CONCLUSION -- ACKNU WLEDGEMENTS -- BIBLIOGRAPHY -- ADDENDUM -- EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS ' -- Introduction -- The identification and signature scheme -- Preprocessing the random number exponentiation -- Cryptanalysls of preprocessing -- The performance of the signature scheme -- References -- A signature with shared verification scheme -- Introduction -- Geometric background -- Signature for a single user -- The scheme -- Implementation and security -- Attacks -- Signature for a group of users -- References -- ON-LINE/OFF-LINE DIGITAL SIGNATURES -- INTRODUCTION -- THE GENERAL CONSTRUCTION -- PROOF OF THE THEORETICAL RESULT -- CONCRETE IMPLEMENTATIONS -- The Basic Implementation -- Shortening the signature -- Further shortening of the signature -- REFERENCES -- On the Classification of Ideal, Secret Sharing Schemes -- Introduction -- Example: The Rank 2 Case -- Open Questions -- Acknowledgments -- References -- DYNAMIC THRESHOLD SCHEME BASED ON THE DEFINITION OF CROSS-PRODUCTIN AN N-DIMENSIONAL LINEAR SPACE.

INTRODUCTION -- THE CHARACTERIZATIONS OF DYNAMIC THRESHOLD/RAMP SCHEMES -- THE DYNAMIC THRESHOLD SCHEME BASED ONTHE DEFINITION OF CROSS-PRODUCT IN N-DIMENSIONAL SPACE -- SECURITY ANALYSIS AND DISCUSSIONS -- CONCLUSION -- REFERENCES -- Secret Sharing Over Infinite Domains*(extended abstract) -- INTRODUCTION -- SECRET SHARING OVER COUNTABLE SETS -- PERFECT ENCRYPTION OVER COUNTABLE SETS -- SECRET SHARING OVER THE REALS -- ACKNOWLEDGEMENTS -- REFERENCES -- Threshold cryptosystems -- Introduction -- Background -- THRESHOSLCDHE MES -- ELGAMALCR YPTOSYSTEM -- Solutions -- THE BASIC IDEA -- USING LAGRANGEIN TERPOLATION FOR MODIFIED SHADOWGENERATION -- USING A GEOMETRY BASED THRESHOLD -- Enhancements -- AVOIDINGG ALOIFSI ELDS -- ANONYMIT -- Proof of security -- Failures with %A -- Conclusion -- ACKNOWLEDGMEN -- REFERENC -- Flexible Access Control with Master Keys -- Introduction -- Hierarchical Keying -- Master Keys -- Expansion -- Implementation -- Summary -- References -- Key Distribution ProtocolforDigital Mobile Communication Systems -- Introduction -- Previous Key Distribution Schemes -- Centralized Key Distribution Protocol -- Public Key Distribution Protocol -- Proposed Key Distribution Protocol -- An

Active Attack to the Key DistributionProtocol -- A Countermeasure Against the Active Attack -- A Structure in the Sending Data -- A Measure to Prevent a Replay Attack -- User Identity Verification -- Conclusions -- Acknowledgements -- References -- A key exchange system based on real quadraticfieldsExtended abstract -- Introduction -- The idea -- Procedures -- The protocol -- Security -- References -- On Key Distribution Systems -- Introduction -- Proposed Criteria -- General -- Passive Adversary -- Malicious Adversary -- Amortized Security -- Some Diffie-Hellman variations -- The original Diffie-Hellman system -- Time dependent Diffie-Hellman variation. Randomized Diffie-Hellman variation.

Sommario/riassunto

CRYPTO is a conference devoted to all aspects of cryptologic research. It is held each year at the University of California at Santa Barbara. Annual meetings on this topic also take place in Europe and are regularly published in this Lecture Notes series under the name of EUROCRYPT. This volume presents the proceedings of the ninth CRYPTO meeting. The papers are organized into sections with the following themes: Why is cryptography harder than it looks?, pseudo-randomness and sequences, cryptanalysis and implementation, signature and authentication, threshold schemes and key management, key distribution and network security, fast computation, odds and ends, zero-knowledge and oblivious transfer, multiparty computation.