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.

2. Record Nr. UNINA9910827650103321

Titolo	Enabling Conditions for Bioenergy Finance and Investment in Colombia
Pubbl/distr/stampa	Paris : , : Organization for Economic Cooperation & Development, , 2022 ©2022
ISBN	92-64-46390-9
Edizione	[1st ed.]
Descrizione fisica	1 online resource (123 pages)
Soggetti	Clean energy investment Colombia
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Foreword -- Abbreviations and acronyms -- Executive summary -- Actions to unlock the opportunity for sustainable bioenergy development -- 1 Energy sector trends and clean energy prospects -- Introduction -- Colombia is rich in natural resources, with large untapped renewable energy potential -- Residues and waste can play a supporting role in clean energy development. -- Bioenergy can help decarbonise the energy mix, which is dominated by fossil fuels -- Power sector development and bioenergy opportunities -- Secure and affordable electricity supply requires more diverse capacity -- Clean energy solutions can help to achieve secure and reliable electricity supply -- Bioenergy capacity additions need a kick-start if they are to reach their potential -- References -- Notes -- 2 Planning and governance for bioenergy development -- Increasing institutional co-ordination will facilitate bioenergy development -- Strategic planning can spell out the opportunities for bioenergy projects -- Bioenergy targets in the clean energy agenda will support project development -- Climate commitments are an opportunity to improve bioenergy capacity -- Electricity planning can do more to facilitate bioenergy capacity additions -- Emphasis should focus on shaping a vision for clean, reliable and affordable electricity -- Facilitating planning and approval can help build up a pipeline of bioenergy projects -- References -- Notes -- 3 Regulatory measures to

improve the case for sustainable bioenergy -- Early bioenergy cogeneration stresses the importance of a clear regulatory framework -- Clarifying the regulatory environment for bioenergy will support greater project development -- Connection rules and procedures can do more to facilitate bioenergy capacity -- Renewable portfolio targets can work with bioenergy projects, rather than against them.
Stronger waste management regulation will encourage greater energy recovery -- The cost of waste disposal directly influences appetite for bioenergy solutions -- Firm disposal rules and higher fees will improve the business case for waste recovery -- References -- Notes -- 4 Improved competition, innovation and finance for bioenergy development -- Fair market competition will improve the business case for bioenergy projects -- The wholesale market is open, but options are limited for some bioenergy projects -- Use of more targeted measures can facilitate bioenergy access to market -- Innovation and capacity building can improve the business case for bioenergy -- Improved access to finance will increase capacity for bioenergy development -- Tackling the cost of finance will support a stronger pipeline of bioenergy projects -- Public funds and blended finance can de-risk projects and leverage private capital -- Capital markets are an untapped opportunity for clean energy development -- References -- Notes -- 5 Insights for enabling greater finance and investment for bioenergy solutions -- Notes -- References -- Notes -- Annex A. Global experiences with bioenergy development -- Brazil: from waste to energy in the cement industry -- Alternative fuel use for cement production in Brazil -- Policy measures to enable co-processing in cement production -- Lessons learned and implications for the Colombian context -- Chile: international collaboration for better waste management -- The Reciclos Organicos programme -- An enabling policy environment for market development -- Lessons learned and implications for the Colombian context -- Colombia: lessons from cogeneration in the sugar industry -- Use of sugar cane for cogeneration activities: the experience of Manuelita -- An enabling policy environment for market development.
Lessons learned and implications for opportunities moving forward -- India: foreign investment for paddy straw to biogas in Punjab -- The Verbio biogas project -- Financing biogas development -- Lessons learned and implications for the Colombia context -- Turkey: biogas production from livestock manure -- The experience of Energrom Energy in developing biogas capacity -- An enabling policy environment for bioenergy market development -- Lessons learned and implications for the Colombian context.

Sommario/riassunto

Colombia has set forth a number of important policy strategies to achieve its clean energy ambitions, including the 2018 Green Growth Policy, the 2019 National Circular Economy Strategy and the 2022 Energy Transition Policy. These strategies all note the role sustainable bioenergy and waste-to-energy can play in supporting decarbonisation objectives. This report looks at the enabling conditions to encourage development of these clean energy solutions and mobilise the necessary finance and investment.