

1. Record Nr.	UNINA9910785247003321
Autore	Chunawalla S. A
Titolo	Contours of retailing management [[electronic resource] /] / S.A. Chunawalla
Pubbl/distr/stampa	Mumbai, : Himalaya Pub. House, 2009
ISBN	1-282-80180-5 9786612801808 1-4416-6151-4 93-5043-432-6 600-00-2724-9
Edizione	[Rev. ed.]
Descrizione fisica	1 online resource (207 p.)
Disciplina	658.87
Soggetti	Retail trade - Management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	COVER; CONTENTS; INTRODUCTION TO RETAILING; RETAIL ORGANISATION; RETAIL THEORIES AND FORMATS; RETAIL PLANNING; STORE LOCATION; STORE DESIGN AND LAYOUT; SUPPLY CHAIN MANAGEMENT (SCM); CUSTOMER SERVICES; PRICING OF MERCHANDISE; ADVERTISING AND PROMOTION; HUMAN RESOURCES IN RETAILING; RETAIL ACCOUNTING; UNDERSTANDING CONSUMER BEHAVIOUR; IT IN RETAILING; BRAND MANAGEMENT IN RETAILING; DISTRIBUTION AND RETAILING; OPERATING A RETAIL BUSINESS; INTERNATIONAL RETAILING
Sommario/riassunto	Indian retailing reminded one of the sweat shops run by half-educated gentlemen and ladies on meagre finance mostly raised by pawing one's family silver or borrowing at exorbitant rates and supplemented by own savings. Goods piled and stacked up haphazardly littered these pigeonholes. The customers were separated from the goods by counter and battalions of salespeople. The whole scene has changed dramatically in the last 10-15 years. We have world-class malls housing swanky stores. The stores are run by highly educated entrepreneurs and well organised corporates. The salespersons are suave, educated

2. Record Nr.	UNISA996589543803316
Autore	Chattopadhyay Anupam
Titolo	Progress in Cryptology - INDOCRYPT 2023 : 24th International Conference on Cryptology in India, Goa, India, December 10-13, 2023, Proceedings, Part I
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2024 ©2024
ISBN	3-031-56232-1
Edizione	[1st ed.]
Descrizione fisica	1 online resource (364 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14459
Altri autori (Persone)	BhasinShivam PicekStjepan RebeiroChester
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	<p>Intro -- Foreword -- Preface -- Organization -- Invited Papers --</p> <p>Secure Boot in Post-Quantum Era -- Patent Landscape in the field of Hash-Based Post-Quantum Signatures -- Contents - Part I --</p> <p>Contents - Part II -- Symmetric-Key Cryptography, Hash Functions, Authenticated Encryption Modes -- Multimixer-156: Universal Keyed Hashing Based on Integer Multiplication and Cyclic Shift -- 1</p> <p>Introduction -- 2 Preliminaries and Notations -- 2.1 and -universality -- 2.2 Key-then-Hash Functions -- 2.3 Parallel Universal Hashing --</p> <p>2.4 Notations -- 2.5 Differential Properties of Integer Multiplication --</p> <p>3 Multimixer-156 -- 3.1 Motivation and Design Rationale -- 3.2</p> <p>Analysis of Bitwise Cyclic Shift -- 3.3 Feistel-with-Rotation and the Rotate-then-Multiply Functions -- 3.4 Specifications of F-156 -- 3.5</p> <p>Maximum Image Probability of F-156 -- 3.6 Maximum Differential Probability of F-156 -- 4 Implementation and Benchmarking Results --</p> <p>References -- On the Security of Triplex- and Multiplex-Type Constructions with Smaller Tweaks -- 1 Introduction -- 1.1 Leakage-Resilient Authenticated Encryption -- 1.2 Security Models for Leakage-Resilient Authenticated Encryption -- 1.3 Revisiting Triplex and Multiplex -- 1.4 Our Contribution -- 2 Preliminaries -- 2.1 Security Notions -- 2.2 Tweakable Block Cipher -- 2.3 Nonce-Based Single-</p>

Pass Authenticated Encryption -- 2.4 (Multi-user) Ciphertext Integrity Under Misuse Leakage -- 2.5 (Multi-user) Chosen-Ciphertext Indistinguishability Under Nonce Misuse and Leakage -- 3 Forgery Complexity on Triplex- and Multiplex-Type Constructions -- 3.1 Forging Attack on Triplex with Smaller Tweak -- 3.2 Forgery Attacks on Multiplex with  $\leq$  dn-bit TBCs -- 4 The Tweplex Authenticated Cipher -- 5 Authentication Security of Tweplex -- 5.1 Query Types and Responses -- 5.2 Defining Bad Events and Bounding Their Probabilities. 6 Confidentiality Analysis of Tweplex -- 6.1 Query Types and Responses -- 6.2 Confidentiality Under Nonce Misuse and Bounded Leakage -- 6.3 Proof Idea of muCCAmL1 Security -- 7 Conclusion -- References -- From Substitution Box to Threshold -- 1 Introduction -- 2 Background -- 2.1 Side Channel Attack and Countermeasure -- 3 Threshold Without Decomposition (Combinational SBox) -- 3.1 Need for a Well-Developed Algorithm -- 3.2 Our Approach -- 3.3 Results -- 4 Threshold with Decomposition (Sequential SBox) -- 5 Further Optimisation Based on Affine Equivalence -- 5.1 Motivation and Basic Observation -- 5.2 Improving Efficiency with Affine Equivalent SBox -- 5.3 Results -- 6 Conclusion -- References -- Tight Security Bound of 2k-LightMAC\_Plus -- 1 Introduction -- 1.1 Beyond Birthday Bound Secure Variants of LightMAC -- 1.2 Our Contribution -- 2 Preliminaries -- 2.1 Psuedorandom Function and Pseudorandom Permutation -- 2.2 Mirror Theory -- 3 Proof of Theorem 1 -- 3.1 Description of the Ideal World -- 3.2 Definition and Probability of Bad Transcripts -- 3.3 Analysis of Good Transcript -- 4 Matching Attack on 2k-LightMAC\_Plus -- 4.1 Attack Idea -- 4.2 Attack Complexity -- 5 Conclusion -- References -- Designing Full-Rate Sponge Based AEAD Modes -- 1 Introduction -- 1.1 Existing Security Bounds for Sponge-Type AEAD Schemes -- 1.2 Our Contributions -- 1.3 Significance of the Result -- 2 Preliminaries -- 2.1 Authenticated Encryption: Definition and Security Model -- 2.2 Coefficients H Technique -- 2.3 Multi-chain Graph -- 3 Full-Rate-Transform-then-Permute AEAD -- 3.1 Revisiting Transform-then-Permute Paradigm -- 3.2 Full-Rate-Transform-then-Permute AEAD with Extra-State -- 3.3 Rationale of the Assumptions on the Feedback Function -- 4 Security of frTtP AEAD with Extra State -- 4.1 Security of Modified ORANGE-Zest. 4.2 (In)security of Full Rate Sponge-Duplex and Oribatida -- 4.3 frTtP with Combined and Beetle Feedback -- 5 Proof of Theorem 2 -- 5.1 Description of the Ideal World -- 5.2 Defining and Bounding Bad Transcripts in Ideal World -- 5.3 Good Transcript Analysis and Completion of the Proof -- 5.4 Conclusion and Future Direction -- References -- Towards Minimizing Tweakable Blockcipher-Based Generalized Feistel Networks -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Blockciphers and Tweakable Blockciphers -- 2.3 Security Definition and H-Coefficient Technique -- 3 Definition of Extended TBC-Based Type-2 GFN -- 4 Birthday SPRP Security at 4 Rounds -- 4.1 Definition of the Oracles -- 4.2 Bad Transcripts and Bad Probability -- 4.3 Analysis of Good Transcripts -- 5 Conclusion -- A Candidate Good Diffusion Layers for Definition 1 -- References -- The Patching Landscape of Elisabeth-4 and the Mixed Filter Permutator Paradigm -- 1 Introduction -- 2 Preliminaries -- 2.1 Boolean Functions and Cryptography -- 2.2 Group Filter Permutator Paradigm -- 2.3 GFP and Security Analysis -- 3 Linearization Attack from ch7ElisabethAttack -- 4 Elisabeth-b -- 5 Gabriel -- 6 Margrethe and Mixed Filter Permutators -- 6.1 Mixed Filter Permutator Paradigm -- 6.2 Margrethe -- 6.3 Security Analysis -- 7 Conclusion and Open Question -- References -- Elliptic Curves, Zero-Knowledge Proof, Signatures -- Generating Supersingular Elliptic Curves over  $\mathbb{F}_p$  with Unknown

Endomorphism Ring -- 1 Introduction -- 2 Definitions and Assumptions -- 3 Existing Solutions -- 3.1 Signature Schemes -- 3.2 Multiparty Key Generation -- 4 A New Zero-Knowledge Proof -- 4.1 Avoiding the Random Oracle Model -- 5 Secure Curve Generation -- 5.1 Generating Secure Curves Without a Random Oracle -- 6 Curve Randomizer -- 7 Conclusion -- References.  
Kummer and Hessian Meet in the Field of Characteristic 2 -- 1  
Introduction -- 1.1 Our Contribution -- 2 Background -- 2.1 Weierstrass Curve -- 2.2 Binary Kummer Line -- 2.3 Binary Generalized Hessian Curve -- 3 Retrieving the R and S-Coordinates of  $nP$  -- 3.1 Retrieve R and S Coordinates -- 4 Moving Between Weierstrass Curve and Generalized Hessian Curve -- 4.1 Moving Between Weierstrass Curve and Triangular Form -- 4.2 Moving Between BEwT(a3) to  $H()$  -- 4.3 Moving Between BEw(b) and  $H()$  via Isomorphism -- 4.4 Moving Between BEw(b) and  $H()$  via Isogeny -- 4.5 Optimized Arithmetic on  $H()$ , 1) -- 5 Concrete Proposal of Curves -- 6 Conclusion -- References -- Synchronized Aggregate Signature Under Standard Assumption in the Random Oracle Model -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Overview of Techniques -- 2 Preliminaries -- 2.1 Bilinear Pairing -- 2.2 Computational Assumptions -- 2.3 Synchronized Aggregate Signature Definition -- 3 Synchronized Aggregation Under Standard Assumption -- 3.1 SynAS Construction -- 3.2 Security of SynAS Scheme -- 4 Comparison -- References -- Malleable Commitments from Group Actions and Zero-Knowledge Proofs for Circuits Based on Isogenies -- 1 Introduction -- 2 Preliminaries -- 2.1 Commitment Scheme -- 2.2 Group Actions -- 2.3 Sigma Protocols -- 2.4 Proof Systems -- 3 Malleable Commitments -- 3.1 A Generic Notion of Malleability -- 4 Malleable Commitments from Group Actions -- 4.1 Commitment Products -- 5 Proof Systems for an Admissible Group-Action Based Commitment -- 5.1 Proof System for Small Message Space -- 5.2 Proof System for Message Spaces with a Subgroup Structure -- 5.3 NIZK via the Fiat-Shamir Transform -- 6 Proof Systems for NP Statements -- 6.1 Arithmetic Circuits over a Small Ring -- 6.2 Proof System for Rank-1 Constraint System over a Small Ring -- 6.3 Zero-Knowledge Proofs for Branching Programs.  
6.4 Discussion and Further Work -- 7 Conclusion -- References -- Attacks -- A CP-Based Automatic Tool for Instantiating Truncated Differential Characteristics -- 1 Introduction -- 2 Tagada -- 2.1 Differential Cryptanalysis -- 2.2 How Tagada Works -- 2.3 First Step Results -- 3 Model Generation for the Second Step -- 3.1 Modelling DDT with Table Constraints -- 3.2 Modelling Other Operators -- 4 Connect the Two Steps -- 5 Second Step Optimizations -- 5.1 Heuristics -- 5.2 Competitive Parallel Solving -- 6 Results -- 7 Conclusion -- 7.1 Next Optimization: DAG Simplification -- 7.2 Future Work -- References -- Falling into Bytes and Pieces - Cryptanalysis of an Apple Patent Application -- 1 Introduction -- 2 Description of ABC -- 2.1 The Round Function of ABC -- 2.2 The Key Schedule -- 3 Cryptanalysis of ABC -- 3.1 Exploiting Lack of Diffusion -- 3.2 Generic Attacks -- 3.3 A Closer Look at S and BS -- 3.4 Differential Cryptanalysis of B2 and B4 -- 4 Key Recovery -- 4.1 Dependencies in the ABC Key Schedule -- 4.2 Recovering the Master Key from kB2 and kB4 -- 5 Conclusion -- References -- Grover on Chosen IV Related Key Attack Against GRAIN-128a -- 1 Introduction -- 2 Preliminaries -- 2.1 Design of GRAIN-128a -- 2.2 Chosen IV Attacks and Chosen IV Related Key Attack -- 2.3 Grover's Search Algorithm -- 3 Classical Chosen IV Related Key Attack on Grain-128a -- 4 Quantum Chosen IV Related Key Attack on Grain-128a Using Grover's Algorithm -- 5 Simulation of the Attack in IBMQ Interface -- 5.1 Structure of Toy-Grain -- 5.2

Experimental Result -- 6 Resource Estimation for Hardware Implementation -- 6.1 Cost of the Attack Under NIST MAXDEPTH Limit -- 7 Conclusion -- References -- Concrete Time/Memory Trade-Offs in Generalised Stern's ISD Algorithm -- 1 Introduction -- 1.1 Previous and Related Works -- 2 Preliminaries -- 2.1 ISD Algorithms from Prange to Stern.  
3 A Generalisation of Stern's ISD Algorithm.

---