1. Record Nr. UNISA996383794903316

Autore	Lydgate John <1370?-1451?>
Titolo	This lytell treatyse compendiously declareth the damage and destruction in realmes [[electronic resource]] : caused by the serpente of diuision
Pubbl/distr/stampa	[London], : Newly and of late imprinted by me Roberte Redman, dwellynge at London in Flete Strete at the sygne of the George, [ca. 1535]
Descrizione fisica	[44] p
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Attributed to Lydgate by STC (2nd ed.). "Thus endeth this lytell treatyse entytuled the Damage and destruction in realmes"--Colophon. Publisher statement taken from colophon; date of imprint suggested by STC (2nd ed.). Signatures: A-Bâ¸ Câ¶. T.p. contains illustration. Reproduction of original in the Exeter College (University of Oxford). Library.
Sommario/riassunto	eebo-0051

2. Record Nr. UNINA9910574074903321

Titolo	Advances in Cryptology – EUROCRYPT 2022 : 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 – June 3, 2022, Proceedings, Part III / / edited by Orr Dunkelman, Stefan Dziembowski
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-031-07082-8
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (841 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13277
Disciplina	005.824 005.82
Soggetti	Cryptography Data encryption (Computer science) Application software Computer networks Data protection Cryptology Computer and Information Systems Applications Computer Communication Networks Security Services Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents - Part III -- Symmetric-Key Cryptanalysis -- Key Guessing Strategies for Linear Key-Schedule Algorithms in Rectangle Attacks -- 1 Introduction -- 2 Generalized Key-Recovery Algorithms for the Rectangle Attacks -- 2.1 Attack I: Biham-Dunkelman-Keller's Attack -- 2.2 Attack II: Biham-Dunkelman-Keller's Attack -- 2.3 Attack III: Zhao et al.'s Related-Key Attack -- 3 Key-Guessing Strategies in the Rectangle Attack -- 3.1 New Related-Key Rectangle Attack with Linear Key Schedule -- 3.2 On the Success Probability and Exhaustive Search Phase -- 4 Automatic Model for SKINNY -- 4.1 Previous Automatic Search Models for Boomerang

Distinguishers on SKINNY -- 4.2 Our Model to Determine the Optimal Distinguisher -- 4.3 Comparisons Between Qin et al.'s Model and Ours -- 4.4 New Distinguishers for SKINNY -- 5 Improved Attacks on SKINNY -- 5.1 Improved Attack on 32-Round SKINNY-128-384 -- 6 Conclusion and Further Disscussion -- References -- A Correlation Attack on Full SNOW-V and SNOW-Vi -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations and Definitions -- 2.2 Description of SNOW-V and SNOW-Vi -- 3 Linear Approximation of SNOW-V -- 4 Automatic Search of Linear Approximation Trails of SNOW-V -- 5 Evaluating the Accurate Correlations for a Special Type of Binary Linear Approximations -- 6 A Correlation Attack on SNOW-V -- 6.1 General Description of the Presented Correlation Attack on SNOW-V -- 6.2 Success Probability and Complexity -- 7 A Correlation Attack on SNOW-Vi -- 7.1 Linear Approximation of SNOW-Vi -- 7.2 Compared with the Linear Approximation of SNOW-V -- 8 Conclusion -- A Detailed Reasoning Process of Intermediate Masks -- B The Proof of d=(0,0,0,0) Under d L =(0x000000*,0,0,0,0x000000*,0,0,0) -- References -- Refined Cryptanalysis of the GPRS Ciphers GEA-1 and GEA-2 -- 1 Introduction.
1.1 First Public Analysis of GEA-1 and GEA-2 -- 1.2 Our Results -- 1.3 Technical Contributions -- 1.4 Structure of the Paper -- 2 Preliminaries -- 2.1 Description of GEA-1 and GEA-2 -- 2.2 Notation -- 2.3 Computation Model and Data Structures -- 2.4 3-XOR Problem -- 2.5 4-XOR Problem -- 3 Memory-Optimized Attack on GEA-1 -- 3.1 Weakness in the GEA-1 Initialization Process -- 3.2 Basic Meet-in-the-Middle Attack -- 3.3 Basic Memory-Optimized Attack -- 3.4 Attack G1 - Improved Memory-Optimized Attack -- 4 Attacks on GEA-2 -- 4.1 Previous Attacks on GEA-2 -- 4.2 Basic 4-XOR Attack -- 4.3 Attack G2-1 - Extended 4-XOR Attack -- 4.4 Attacks Targeting the GEA-2 Initialization -- References -- .26em plus .1em minus .1emRevamped Differential-Linear Cryptanalysis on Reduced Round ChaCha -- 1 Introduction -- 2 Structure of ChaCha -- 3 Idea of Differential-Linear Cryptanalysis -- 3.1 Choosing a Right Pair -- 3.2 Probabilistic Neutral Bits -- 3.3 Complexity Computation -- 4 Modification in the Criteria for a Right Pair -- 5 Modification of the Time Complexity Estimation -- 6 Improving the PNBs -- 7 Construction of Memory -- 7.1 Decomposition into Memory and Non-memory Subspace -- 7.2 How to Construct the Attack -- 8 Attack on 7-round ChaCha256 -- 8.1 Practical Observations to Confirm the Theoretical Estimations -- 9 Results on ChaCha128 -- 9.1 Attack on 6.5-round ChaCha128 -- 9.2 Attack on 6-round ChaCha128 -- 10 Conclusion -- References -- A Greater GIFT: Strengthening GIFT Against Statistical Cryptanalysis -- 1 Introduction -- 1.1 Our Results -- 2 Preliminary -- 2.1 Specification of GIFT-64 -- 2.2 Bit Permutation in PermBits Operation of GIFT-64 -- 2.3 Accelerated Automatic Search with the SAT Method -- 3 Differential Property of GIFT-64 -- 3.1 Observations on Experimental Results -- 3.2 Lifted Bounds on the Number of Differential Active S-boxes.
3.3 Decreased Upper Bound on the Differential Probability -- 3.4 Alternative Description for the Round Function of GIFT-64 -- 3.5 Differential Characteristics with Two Active S-boxes per Round -- 3.6 Enumerating All Optimal Differential Characteristics -- 4 Linear Property of GIFT-64 -- 4.1 Fluctuant Bounds in Linear Cryptanalysis Setting -- 4.2 Linear Characteristics with Two Active S-boxes per Round -- 5 Can We Improve GIFT-64? -- 5.1 Candidate Variants -- 5.2 Classifying the Variants of GIFT-64 -- 5.3 Differential and Linear Properties of GIFT-64-like Ciphers -- 5.4 Properties of Variants in GIFT-64[2021] -- 6 Conclusion and Future Work -- 6.1 Conclusion -- 6.2 Future Work -- References -- Side Channel Attacks and Masking --

Approximate Divisor Multiples - Factoring with Only a Third of the Secret CRT-Exponents -- 1 Introduction -- 2 Coppersmith's Method -- 3 Our Two-Step Partial Key Exposure Attack -- 3.1 Step 1: Computing (k,), Given MSBs -- 3.2 Step 1: Computing (k,), Given LSBs -- 3.3 Step 2: Factoring N, Given k -- 3.4 On the Limits of Improving Our Attack -- 4 Limits of the Takayasu-Kunihiro PKE for Small e -- 4.1 Why TK Fails for e N1/8 -- 5 Experimental Results -- References -- Information-Combining Differential Fault Attacks on DEFAULT -- 1 Introduction -- 2 Background -- 2.1 Differential Fault Analysis -- 2.2 Design and Specification of DEFAULT -- 3 Information-Combining DFA on Simple Key Schedule -- 3.1 Limited Information Learned via DFA -- 3.2 Basic Encrypt-Decrypt Attack on Simple Key Schedule -- 3.3 Basic Multi-round Attack on Simple Key Schedule -- 4 Exploiting Equivalence Classes of Keys -- 4.1 Equivalent Keys in the DEFAULT Framework -- 4.2 Normalized Keys -- 4.3 Generic Attack Strategy for Ciphers with Linear Structures -- 5 Information-Combining DFA on Rotating Key Schedule.
5.1 Basic Encrypt-Decrypt Attack on Rotating Key Schedule -- 5.2 Basic Multi-round Attack on Rotating Key Schedule -- 6 Reducing the Number of Faults -- 6.1 Optimized Encrypt-Decrypt Attack on Simple Key Schedule -- 6.2 Optimized Multi-round Attack on Simple Key Schedule -- 6.3 Optimized Multi-round Attack on Rotating Key Schedule -- 7 Discussion -- 8 Conclusion -- References -- Private Circuits with Quasilinear Randomness -- 1 Introduction -- 1.1 Our Contribution -- 2 Technical Overview -- 2.1 Outer Construction: Private Circuits via Leakage-Tolerant XOR Gadgets -- 2.2 Inner Construction and Robust Parity Sharing Generator -- 2.3 Extensions -- 3 Preliminaries -- 3.1 Private Circuits -- 3.2 Strong t-wise Independent Pseudo-Random Generator -- 4 Outer Construction: t-private Circuit via Leakage-Tolerant XOR Gadgets -- 5 Inner Construction: Leakage-Tolerant XOR Gadget -- 5.1 Basic Construction via Correlated Randomness -- 5.2 Robust Parity Sharing Generator -- 6 Construction of Multi-phase Robust Parity Sharing Generator -- References -- Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon -- 1 Introduction -- 2 Preliminaries -- 2.1 Linear Algebra and Lattices -- 2.2 Power-of-Two Cyclotomic Fields -- 2.3 Matrices of Algebraic Numbers and NTRU Modules -- 2.4 Gaussians over Rings -- 3 Sampling Discrete Gaussians in R-Modules -- 3.1 Peikert's Sampler -- 3.2 Ducas and Prest's Hybrid Sampler -- 3.3 An Integer Arithmetic Friendly Sampler -- 3.4 Asymptotic Security of the Samplers -- 3.5 The Mitaka Signature Scheme -- 4 Improved Trapdoor Generation -- 5 Security Analysis of Mitaka -- 6 Implementation Results -- 7 Side-Channel Countermeasure -- 7.1 Preliminaries on Masking Countermeasure -- 7.2 Two New Gadgets -- 7.3 Masking the MitakaZ Sampler -- 7.4 Masking the Mitaka Samplers -- 8 Conclusion -- References.
A Novel Completeness Test for Leakage Models and Its Application to Side Channel Attacks and Responsibly Engineered Simulators -- 1 Introduction -- 1.1 State of the Art -- 1.2 Our Contributions -- 2 Preliminaries -- 2.1 Notation and Background to Leakage Modelling -- 2.2 Leakage Modelling: Approaches -- 2.3 Judging Model Quality -- 2.4 Leakage Certification Techniques -- 3 Model Quality: Is My Leakage Model Complete? -- 3.1 Completeness -- 3.2 Collapsed F-Test for Completeness -- 3.3 Statistical Power of the Nested F-Test -- 4 Dissecting Attacks: Towards Worst-Case Adversaries -- 5 Application to Leakage Simulators -- 5.1 Modelling Leakage of Individual Instructions -- 5.2 Modelling Leakage of Complex Instruction Sequences -- 6 Ethical Considerations and Conclusions -- A PI, HI and

Assumption Error -- A.1 Estimating ``Assumption Errors'' -- A.2 HI and PI -- A.3 Bias-Variance Decomposition -- References -- Towards Micro-architectural Leakage Simulators: Reverse Engineering Micro-architectural Leakage Features Is Practical -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Methodology and Paper Organisation -- 2 Step 1: Identifying Safe Architectural Assumptions -- 3 Step 2: Recovering Major Micro-architectural Leakage Elements -- 3.1 Fetch -- 3.2 Decode -- 3.3 Execute -- 3.4 Register Write-Back -- 3.5 Memory Sub-system -- 4 Step 3: Refining the Micro-architectural Leakage Model -- 4.1 Considering Components with Stable Signals -- 4.2 Glitch and Multiplexer -- 4.3 Putting It All Together -- 5 Putting Our Micro-architectural Model to the Test -- 5.1 Exploiting Decoding Port Leakage -- 5.2 Consequences of Incorrectly Assigning Pipeline Registers -- 5.3 Towards a Micro-architectural Simulator: Elmo -- 6 Conclusion -- References -- Post-Quantum Cryptography -- Beyond Quadratic Speedups in Quantum Attacks on Symmetric Schemes -- 1 Introduction.
2 Classical Constructions and Previous Results.

Sommario/riassunto

The 3-volume-set LNCS 13275, 13276 and 13277 constitutes the refereed proceedings of the 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Eurocrypt 2022, which was held in Trondheim, Norway, during 30 May – 3 June, 2022. The 85 full papers included in these proceedings were accepted from a total of 372 submissions. They were organized in topical sections as follows: Part I: Best Paper Award; Secure Multiparty Computation; Homomorphic Encryption; Obfuscation; Part II: Cryptographic Protocols; Cryptographic Primitives; Real-World Systems Part III: Symmetric-Key Cryptanalysis; Side Channel Attacks and Masking, Post-Quantum Cryptography; Information-Theoretic Security.