1. Record Nr. UNINA9910578688703321

Titolo	Applied cryptography and network security : 20th International Conference, ACNS 2022, Rome, Italy, June 20-23, 2022, proceedings / / edited by Giuseppe Ateniese and Daniele Venturi
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-09234-1
Descrizione fisica	1 online resource (916 pages)
Collana	Lecture Notes in Computer Science ; ; v.13269
Disciplina	005.82
Soggetti	Computer networks - Security measures Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Encryption -- Keyed-Fully Homomorphic Encryption Without Indistinguishability Obfuscation -- 1 Introduction -- 1.1 Background -- 1.2 Contribution -- 1.3 Technical Overview -- 2 Preliminaries -- 2.1 Non-Interactive Zero-Knowledge Argument -- 2.2 Dual-System Simulation-Sound NIZK -- 2.3 (Keyed-)Fully Homomorphic Encryption -- 3 Generic Construction of Keyed-FHE -- 4 Strong DSS-NIZK from Smooth PHPS and Unbounded Simulation-Sound NIZK -- 5 Feasibility of Our Construction -- References -- A Performance Evaluation of Pairing-Based Broadcast Encryption Systems -- 1 Introduction -- 2 An ElGamal Baseline and Other Related Works -- 3 Broadcast Encryption Implementations and Analysis -- 3.1 Boneh-Gentry-Waters Scheme Using Asymmetric Pairings -- 3.2 Gentry-Waters: A Semi-static Variant of the BGW System -- 3.3 Waters Dual System Broadcast Encryption System -- 3.4 Comparison of General Broadcast Encryption Systems -- 4 Applications of Broadcast Encryption -- References -- An Optimized GHV-Type HE Scheme: Simpler, Faster, and More Versatile -- 1 Introduction -- 2 Preliminaries -- 2.1 Cryptographic Problem -- 2.2 Trapdoor Sampling Algorithms -- 2.3 The Gentry-Halevi-Vaikuntanathan Encryption Scheme -- 2.4 Other Preliminaries -- 3 Efficiency Analyses of GHV -- 3.1 On the Density of Trapdoor Matrix Pair (T, T-1) -- 3.2 Theoretical

Efficiency of GHV -- 4 Our Optimized GHV-Type Encryption Scheme -- 4.1 Using a Sparse Matrix to Replace T-1 -- 4.2 Generic Construction of oGHV -- 4.3 Homomorphic Operations and Concrete Parameters -- 4.4 Computational Optimizations -- 4.5 Property Analysis -- 5 Conclusions -- References -- Attacks -- Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle -- 1 Introduction -- 2 Preliminaries -- 2.1 Notations -- 2.2 Cryptographic Components -- 2.3 Authenticated Encryption.
3 Analysis of GIFT-COFB -- 3.1 Our Attack -- 3.2 Brief Analysis on Security Proof -- 4 Analysis of Photon-Beetle -- 4.1 Claimed Security Bound and Our Attack -- 4.2 Analysis of the Bound in ch4ToSC: ChaJhaNan20 -- 4.3 Related-Key Attack -- 5 Conclusions -- A Specifications of GIFT-COFB and Photon-Beetle -- References -- Beware of Your Vibrating Devices! Vibrational Relay Attacks on Zero-Effort Deauthentication -- 1 Introduction -- 2 Background: ZEBRA Review -- 3 Overview and Threat Model -- 4 Design and Implementation -- 4.1 Implementation of ZEBRA -- 4.2 Implementation of Relay Attack -- 4.3 Design of VibRaze's Attack Scenarios -- 5 Data Collection -- 6 Analysis and Results -- 6.1 Performance of ZEBRA -- 6.2 Performance of VibRaze Against ZEBRA -- 7 Potential Mitigations -- 8 Related Work -- 9 Conclusion and Future Work -- References -- ZLeaks: Passive Inference Attacks on Zigbee Based Smart Homes -- 1 Introduction -- 2 Background and Motivation -- 2.1 Zigbee Overview -- 2.2 System and Threat Model -- 3 Passive Inference Attacks on Zigbee -- 3.1 Attack Overview -- 3.2 Passive Network Mapping -- 3.3 Device and Event Identification Using Inferred APL Command -- 3.4 Device Identification Using Periodic Reporting Patterns -- 4 Experimental Setup and Results -- 4.1 Automating Passive Inference Attacks with ZLeaks Tool -- 4.2 Experimental Setup -- 4.3 Evaluation Metrics -- 4.4 Device and Event Identification Using Inferred APL Command -- 4.5 Device Identification Using Periodic Reporting Patterns -- 5 Discussion and Related Work -- 5.1 Security Implications of Leaked Data -- 5.2 Potential Countermeasures -- 5.3 Related Work -- 6 Conclusion -- References -- Passive Query-Recovery Attack Against Secure Conjunctive Keyword Search Schemes -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Searchable Symmetric Encryption.
3.2 Considered Conjunctive Keyword Search Model -- 3.3 Attacker Model -- 3.4 Attacker Knowledge -- 4 CKWS-Adapted Refined Score Attack -- 4.1 Score Attacks -- 4.2 Generic Extension -- 4.3 Transform Key Steps of Refined Score Attack -- 4.4 Revised Algorithm -- 4.5 Complexity -- 5 Experiments -- 5.1 Setup -- 5.2 Results -- 6 Discussion -- 7 Conclusion -- References -- Gummy Browsers: Targeted Browser Spoofing Against State-of-the-Art Fingerprinting Techniques -- 1 Introduction -- 2 Background and Related Work -- 2.1 Browser Fingerprinting -- 2.2 Representative Fingerprinting Techniques -- 2.3 Applications of Browser Fingerprinting -- 3 Attack Model and Spoofing Methods -- 3.1 Attack Model -- 3.2 Spoofing Methods -- 4 Attack Implementation -- 4.1 Acquiring User Browser Fingerprint -- 4.2 Visual Attack -- 4.3 Algorithm Attack: Attacking Prominent Fingerprinting Based Techniques -- 5 Dataset and Evaluation Methodology -- 5.1 FP-Stalker Dataset -- 5.2 Evaluation Methodology -- 6 Results -- 6.1 Visual Attack Results -- 6.2 Algorithm Attack Results -- 7 Implications of Our Attack -- 8 Discussion -- 9 Conclusion -- References -- Identifying Near-Optimal Single-Shot Attacks on ICSs with Limited Process Knowledge -- 1 Introduction -- 2 Background -- 2.1 Closed Control Loops -- 2.2 Process Knowledge Data Sources -- 3 Identifying Near-Optimal Single-Shot Attacks -- 3.1

System Model -- 3.2 Attacker Model -- 3.3 Research Questions and Challenges -- 3.4 Identifying Near-Optimal Single-Shot Attacks in CCL Graphs -- 3.5 Motivating Example -- 4 Implementation -- 5 Experimental Evaluation -- 5.1 Tennessee Eastman Plant -- 5.2 Experimental Attacks -- 6 Discussion -- 7 Related Work -- 8 Conclusion -- References -- RSA Key Recovery from Digit Equivalence Information -- 1 Introduction -- 2 Background -- 2.1 RSA -- 2.2 Fixed-Window Exponentiation.
2.3 Attacks on Fixed-Window Exponentiation -- 2.4 The Heninger-Shacham Algorithm -- 2.5 Markov Chains -- 3 Attacker Model -- 4 Our Approach -- 4.1 Algorithm Overview -- 4.2 Complexity Analysis of the Aligned Case -- 4.3 Independent Markov Chains -- 4.4 Unaligned Case -- 5 Results and Comparisons -- 5.1 Theoretical Results -- 5.2 Experimental Results -- 6 Conclusions -- References -- Practical Seed-Recovery of Fast Cryptographic Pseudo-Random Number Generators -- 1 Introduction -- 2 Description of Arrow -- 3 Attacks on Arrow -- 3.1 Simple Guess-and-Determine Attack on Arrow-II -- 3.2 Longer Guess-and-Determine Attack on Arrow-I -- 3.3 An Attack Against Arrow-III, the Software Version of Arrow -- 4 Description of Trifork -- 5 Attack on Trifork -- 5.1 Recovering Z-r3 -- 5.2 Recovering Y-r2 -- References -- Autoguess: A Tool for Finding Guess-and-Determine Attacks and Key Bridges -- 1 Introduction -- 2 Preliminaries -- 2.1 Guess-and-Determine Technique -- 2.2 Key-Bridging Technique -- 2.3 Connection Relations -- 2.4 A Naive Guess-and-Determine Approach -- 3 Constraint Programming for GD and Key-Bridging -- 3.1 Modelling Knowledge Propagation -- 3.2 Encoding Using CP -- 4 From Guess Basis to Gröbner Basis -- 5 Autoguess -- 5.1 Preprocessing Phase -- 5.2 Early-Abort Technique -- 6 Application to Automatic Search for Key Bridges -- 6.1 Application to PRESENT -- 6.2 Application to LBlock with Nonlinear Key Schedule -- 7 Application to GD Attack on Block Ciphers -- 7.1 Automatic GD Attack on AES -- 8 Application to GD Attack on Stream Ciphers -- 8.1 Automatic GD Attack on ZUC -- 9 Key-Recovery-Friendly Distinguishers -- 9.1 DS-MITM Attack on SKINNY-{64-192, 64-128, 128-256} -- 9.2 Improved DS-MITM Attack on TWINE-80 -- 10 Conclusion -- References -- Cryptographic Protocols -- KEMTLS with Delayed Forward Identity Protection in (Almost) a Single Round Trip.
1 Introduction -- 1.1 Contributions -- 2 Preliminaries -- 3 Protocol -- 4 Security Model -- 5 Security Analysis -- 6 Discussion -- 7 Implementation -- 8 Benchmarking -- References -- Improving the Privacy of Tor Onion Services -- 1 Introduction -- 1.1 Related Work -- 2 Attacks -- 2.1 Tor and Hidden Service Directories -- 2.2 Attacks Targeting Clients -- 2.3 Attacks Targeting Onion Services -- 3 PIR for Descriptor Lookups -- 4 Privacy Analysis for PIR Schemes -- 5 Benchmarking and Results -- 5.1 Hardware-Assisted PIR Benchmarks -- 5.2 CPIR Microbenchmarks -- 5.3 Tor Integration Results -- 6 Conclusion -- References -- Privacy-Preserving Authenticated Key Exchange for Constrained Devices -- 1 Introduction -- 1.1 Related Work -- 1.2 Contributions -- 2 Description of the SAKE Protocol -- 2.1 SAKE -- 2.2 SAKE-AM -- 3 A Flawed Proposal -- 3.1 Issues -- 3.2 Countermeasures -- 4 Security Model -- 4.1 Execution Environment -- 4.2 Security Definitions of the Building Blocks -- 5 Privacy-Preserving SAKE/SAKE-AM -- 6 Security of Privacy-Preserving SAKE/SAKE-AM -- 7 Conclusion -- References -- Relations Between Privacy, Verifiability, Accountability and Coercion-Resistance in Voting Protocols -- 1 Introduction -- 2 Related Work -- 3 Preliminaries -- 3.1 Protocols -- 3.2 Notation Related to Voting Protocols -- 3.3 Verifiability and Accountability -- 3.4 Privacy and Coercion-Resistance -- 4 Relations

		Between Definitions -- 4.1 Coercion-Resistance and Privacy -- 4.2 Accountability and Verifiability -- 4.3 Privacy and Verifiability -- 4.4 Verifiability and Coercion-Resistance -- 4.5 Privacy and Accountability -- 5 Conclusions and Future Work -- References -- System Security -- An Approach to Generate Realistic HTTP Parameters for Application Layer Deception -- 1 Introduction -- 2 Method -- 2.1 Data Collection and Training -- 2.2 Generation of Parameter Names. 3 Evaluation.
2.	Record Nr.	UNINA9910777303103321
	Autore	Moltz Barry J
	Titolo	Bounce! [[electronic resource]] : failure, resiliency, and confidence to achieve your next great success / / Barry J. Moltz
	Pubbl/distr/stampa	Hoboken, N.J., : John Wiley & Sons, c2008
	ISBN	1-281-28472-6 9786611284725 0-470-25717-2
	Descrizione fisica	1 online resource (258 p.)
	Disciplina	650.1
	Soggetti	Business failures Success in business Success
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Bounce!: Failure, Resiliency, and Confidence to Achieve Your Next Great Success; Contents; Preface; Acknowledgments; Chapter 1: Get Ready for Adventure: You Have Never Heard a Speaker Like This Before; Talk the Talk; The Ultimate Reality Show; The Comeback: See, Dreams Can Come True; A Messy Process; Chapter 2: Archetypes of Success: Be Careful What You Wish For; Archetype One: Making Something from Nothing or At Least Not Much; Archetype Two: The Rich Get Richer; Archetype Three: The Comeback-Rocky Revisited; Danger Ahead: Focusing on These Archetypal Outcomes Can Sting Copycats Need Not Apply But Wait-Doesn't Success Breed Success?;

Failure at the Very Top; The Roulette Wheel of Success; Chapter 3: I've Got Your One-Hit Wonder: 867-5309; Chapter 4: The World from Here: Start Where You Are; The "Failure Is Not an Option" Cultures; What a GEM!; Laws Affecting Business Reflect Cultural DNA; Chapter 5: Forget the Archetypes: Messy Lines Teach Humility; Have Humility or Have It Bestowed upon You; My Mother's Model of Success; Cycle the Random Walk; Skate the Random Walk; A Call from Your Three Sisters; More Bad Weather Ahead: Blame-Storming
Is There a Formula for Humility? The Ego Is Dead-Or Is It?; Can We Dress Up the Ego and Pretend?; These Egos Have Left the Building without Humility; Humility Tells Us That We Are Not Our Businesses; Humility: Let's Talk about Mistakes; The Tylenol Drug Scare; Humility Allows Us to Learn from Mistakes-Sometimes; Humility Balances Ego; Chapter 6: Failure Is an Option: Flying Fear in Formation; Greet Failure with a New Vocabulary; Meet Failure's Close Relative, Fear; Fear of Being Different and Not as Successful as I Ought to Be; The Elements Called Success and Failure; FUD Takes Hold
Skip the Logo Design, Take a Step Fear of Failure Can Motivate, and Then It's Not All Bad; Facing Your Fear: Jump!; Teaching Butterflies to Fly in Formation; With Failure and Fear Comes Choice; Chapter 7: Embracing Failure When It Happens; Reverse-Engineering Our Past; Oh, What a Shame; Forgive Others-And Then Yourself; Moving Outcomes: Owning Our Mistakes; This Thing We Call Failure; Embracing Failure: An Acquired Taste; Like Success, Failure Is Part of the Cycle of Business; Letting Go of the Embrace; Written All over Your Face; Chapter 8: Failure Provides Choices; Lost? Try the Escape Hatch
Getting to No Dynamic Learners; Morphing into Your Next Success; Start from Where You Are, Right Now; Patient Passion-Choose Intensity; Passion, Confidence, and the Bottomless Bounce; Chapter 9: Do It Anyway: Be a Smart Risk Taker; Chapter 10: A Little DAB will Do Ya! Drive, Accept, and Build; It's All about the Process, Dilbert; Earning Your License to Fail; Chapter 11: Goal Setting: Establishing Your Own Scorecard; Make Progress via Intermediate Goals; Define the Goal before You Start: Striving for Minimal Achievement; Patient Dreams; Raising That White Flag: No Shame in Surrender
Having Too Much Will Make You Stupid

Sommario/riassunto

Conventional business wisdom tells you that there's always something to learn from failure. Not true, says Barry Moltz. Sometimes, failure just stinks. Bounce! explains how success and failure are simply normal outcomes in the regular lifecycle of a business and that process over the long term matters far more than individual outcomes. This book shows you how to build a business that can "bounce" through these cycles for long-term success. If you run a business, better make it Bounce!

3. Record Nr. UNINA9910815801803321

Autore	Nida Eugene A (Eugene Albert), <1914-2011.>
Titolo	Fascinated by languages / / Eugene A. Nida
Pubbl/distr/stampa	Amsterdam ; ; Philadelphia, : J. Benjamins Pub. Co., c2003
ISBN	1-282-16114-8 9786612161148 90-272-9641-3
Edizione	[1st ed.]
Descrizione fisica	1 online resource (163 p.)
Disciplina	418/.02
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references (p. [145]-151) and index.
Nota di contenuto	Fascinated by Languages -- Title page -- LCC page -- Contents -- Fascinated by languages -- Part I: In more than ninety countries -- Travel surprises -- Africa South of the Sahara -- Asia -- Latin America -- North America -- Eastern Europe -- Western Europe -- Part II: Bible translation, texts and interpretations -- Bible translation -- Bible as literary genre -- Texts and interpretations -- Specific Bible translation problems -- Part III: A personal touch -- Who am I? -- Selective Bibliography -- Index.
Sommario/riassunto	In this unique account of 60 years of Bible translation, Eugene Nida sets out his journey with a personal touch. On the way, he reveals the importance of a solid knowledge of Greek and Hebrew as well as of the historical settings in which the Bible was created, in order to render effective translations. Through his story we get to know Nida's views on translations through the ages, in different cultures and narrative traditions, right through to the 21st Century.This book is in the first place a study in anthropological linguistics that tells the rich history of Bible translation, the Bible Societies, translator training, and cultural translation problems.Eugene A. Nida (1914) went to UCLA (Phi Beta Kappa, 1936) and the University of Southern California (Helenistic Greek, 1939). He taught at the Summer Institute of Linguistics from 1937-1952 and is past president of the Linguistic Society of America (1968).From 1943-1981 he was language consultant for the American

Bible Society and the United Bible Societies which led him to study many cultures across 96 countries and to lecture in over a hundred universities and colleges to this day.His published works include Bible Translating (1946), Customs and Cultures (1954), Toward a Science of Translating (1964), Religion across Cultures (1968), The Sociolinguistics of Intercultural Communication (1996) and Translation in Context (2002).