Access Free Information Security And Cryptology Icisc 2017 20th International Conference Seoul South Korea November 29 December 1 2017 Revised Selected Papers Lecture Notes In Computer Science Free Download Pdf

Information Security and Cryptology – ICISC 2017 Information Security and Cryptology – ICISC 2018 Information Security and Cryptology – ICISC 2019 Information Security and Cryptology – ICISC 2021 Information Security and Cryptology – ICISC 2020 IoT Security IoT Security Information Security Applications Side Channel Attacks Cryptology and Network Security Information and Communications Security Progress in Cryptology – INDOCRYPT 2019 Progress in Cryptology – INDOCRYPT 2021 Information Security and Cryptology Computational Science and Technology Advances in Cryptology – ASIACRYPT 2020 Information Security and Cryptology – ICISC 2016 Progress in Cryptology – LATINCRYPT 2019 Progress in Cryptology – AFRICACRYPT 2018 Searchable Encryption Information Security and Privacy Cryptographic Security Solutions for the Internet of Things Education, Research and Business Technologies Interactions between Group Theory, Symmetry and Cryptology Blockchain: Empowering Secure Data Sharing VLSI and Hardware Implementations using Modern Machine Learning Methods Security and Cryptography for Networks Advances in Cryptology – EUROCRYPT 2020 Advances in Cryptology – ASIACRYPT 2021 Provable and Practical Security Selected Areas in Cryptography – SAC 2019 Advances in Cryptology –

EUROCRYPT 2019 Boolean Functions for Cryptography and Coding Theory Advances in Cryptology – CRYPTO 2019 Advances in Cryptology – EUROCRYPT 2018 Verifiable Composition of Signature and Encryption Protocols for Authentication and Key Establishment Security, Privacy, and Applied Cryptography Engineering The 8th International Conference on Computer Engineering and Networks (CENet2018) E-Business and Telecommunications

This book constitutes the refereed proceedings of the 22nd International Conference on Cryptology in India, INDOCRYPT 2021, which was held in Jaipur, India, during December 12-15, 2021. The 27 full papers included in these proceedings were carefully reviewed and selected from 65 submissions. They were organized in topical sections as follows: authenticated encryption; symmetric cryptography; lightweight cryptography; side-channel attacks; fault attacks; post-quantum cryptography; public key encryption and protocols; cryptographic constructions; blockchains. This book constitutes the refereed proceedings of the 9th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2019, held in Gandhinagar, India, in December 2019. The 12 full papers presented were carefully reviewed and selected from 24 submissions. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is a very challenging field, requiring the expertise from diverse domains, ranging from mathematics to solid-state circuit design. This book constitutes the thoroughly refereed post-conference proceedings of the 19th International Conference on Information Security Applications, WISA 2018, held on Jeju Island, Korea, in August 2018. The 11 revised full papers and 11 short papers presented in this volume were carefully reviewed and selected from 44 submissions. #The primary focus of WISA 2018 was on systems and network security including all other technical and practical aspects of security applications and also on the embedded, unmanned or autonomous systems and cyber physical systems in general. This book constitutes revised selected papers from the 20th International Conference on Information Security and Cryptology, ICISC 2017, held in Seoul, South Korea, in November/December 2017. The total of 20 papers presented in this volume were carefully reviewed and selected from 70 submissions. The papers were organized in topical sections named: symmetric key encryption; homomorphic encryption, side channel analysis and implementation; broadcast encryption; elliptic curve; signature and

protocol; and network and system security. The three-volume proceedings LNCS 12491, 12492, and 12493 constitutes the proceedings of the 26th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2020, which was held during December 7-11, 2020. The conference was planned to take place in Daejeon, South Korea, but changed to an online format due to the COVID-19 pandemic. The total of 85 full papers presented in these proceedings was carefully reviewed and selected from 316 submissions. The papers were organized in topical sections as follows: Part I: Best paper awards; encryption schemes.- post-quantum cryptography; cryptanalysis; symmetric key cryptography; message authentication codes; side-channel analysis. Part II: public key cryptography; lattice-based cryptography; isogeny-based cryptography; quantum algorithms; authenticated key exchange. Part III: multi-party computation; secret sharing; attribute-based encryption; updatable encryption; zero knowledge; blockchains and contact tracing. This book constitutes the proceedings of the 11th International Conference on Security and Cryptography for Networks, SCN 2018, held in Amalfi, Italy, in September 2018. The 30 papers presented in this volume were carefully reviewed and selected from 66 submissions. They are organized in topical sections on signatures and watermarking; composability; encryption; multiparty computation; anonymity and zero knowledge; secret sharing and oblivious transfer; lattices and post quantum cryptography; obfuscation; two-party computation; and protocols. With the development of big data, data sharing has become increasingly popular and important in optimizing resource allocation and improving information utilization. However, the expansion of data sharing means there is an urgent need to address the issue of the privacy protection – an area where the emerging blockchain technology offers considerable advantages. Although there are a large number of research papers on data sharing modeling and analysis of network security, there are few books dedicated to blockchain-based secure data sharing. Filing this gap in the literature, the book proposes a new data-sharing model based on the blockchain system, which is being increasingly used in medical and credit reporting contexts. It describes in detail various aspects of the model, including its role, transaction structure design, secure multi-party computing and homomorphic encryption services, and incentive mechanisms, and presents corresponding case studies. The book explains the security architecture model and the practice of building data sharing from the blockchain infrastructure, allowing readers to understand the importance of

data sharing security based on the blockchain framework, as well as the threats to security and privacy. Further, by presenting specific data sharing case studies, it offers insights into solving data security sharing problems in more practical fields. The book is intended for readers with a basic understanding of the blockchain infrastructure, consensus mechanisms, smart contracts, secure multiparty computing, homomorphic encryption and image retrieval technologies. This book constitutes revised selected papers from the 21st International Conference on Information Security and Cryptology, ICISC 2018, held in Seoul, South Korea, in November 2018. The total of 21 papers presented in this volume were carefully reviewed and selected from 49 submissions. The papers were organized in topical sections named: public-key encryption and implementation; homomorphic encryption; secure multiparty computation; post-quantum cryptography; secret sharing and searchable encryption; storage security and information retrieval; and attacks and software security. This book includes high-quality research papers presented at 20th International Conference on Informatics in Economy (IE 2021), which is held in Bucharest, Romania during May 2021. The book covers research results in business informatics and related computer science topics, such as IoT, mobile-embedded and multimedia solutions, e-society, enterprise and business solutions, databases and big data, artificial intelligence, data-mining and machine learning, quantitative economics. This book constitutes the refereed proceedings of the 10th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICACRYPT 2018, held in Marrakesh, Morocco, in May 2018. The 19 papers presented in this book were carefully reviewed and selected from 54 submissions. AFRICACRYPT is a major scientific event that seeks to advance and promote the field of cryptology on the African continent. The conference has systematically drawn some excellent contributions to the field. The conference has always been organized in cooperation with the International Association for Cryptologic Research (IACR). This book constitutes selected papers from the 23rd International Conference on Information Security and Cryptology, ICISC 2020, held in Seoul, South Korea, in December 2020. Due to the COVID-19, the confere was held online. The total of 15 papers presented in this volume were carefully reviewed and selected from 51 submissions. The aim of this conference was to provide an international forum for the latest results of research, development, and applications within the field of information security and cryptology. This monograph gives a thorough treatment of the celebrated

compositions of signature and encryption that allow for verifiability, that is, to efficiently prove properties about the encrypted data. This study is provided in the context of two cryptographic primitives: (1) designated confirmer signatures, an opaque signature which was introduced to control the proliferation of certified copies of documents, and (2) signcryption, a primitive that offers privacy and authenticity at once in an efficient way. This book is a useful resource to researchers in cryptology and information security, graduate and PhD students, and security professionals. This Special Issue provides an opportunity for researchers in the area of side-channel attacks (SCAs) to highlight the most recent exciting technologies. The research papers published in this Special Issue represent recent progress in the field, including research on power analysis attacks, cache-based timing attacks, system-level countermeasures, and so on. Machine learning is a potential solution to resolve bottleneck issues in VLSI via optimizing tasks in the design process. This book aims to provide the latest machine-learning–based methods, algorithms, architectures, and frameworks designed for VLSI design. The focus is on digital, analog, and mixed-signal design techniques, device modeling, physical design, hardware implementation, testability, reconfigurable design, synthesis and verification, and related areas. Chapters include case studies as well as novel research ideas in the given field. Overall, the book provides practical implementations of VLSI design, IC design, and hardware realization using machine learning techniques. Features: Provides the details of state-of-the-art machine learning methods used in VLSI design Discusses hardware implementation and device modeling pertaining to machine learning algorithms Explores machine learning for various VLSI architectures and reconfigurable computing Illustrates the latest techniques for device size and feature optimization Highlights the latest case studies and reviews of the methods used for hardware implementation This book is aimed at researchers, professionals, and graduate students in VLSI, machine learning, electrical and electronic engineering, computer engineering, and hardware systems. The four-volume proceedings LNCS 13090, 13091, 13092, and 13093 constitutes the proceedings of the 27th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2021, which was held during December 6-10, 2021. The conference was planned to take place in Singapore, but changed to an online format due to the COVID-19 pandemic. The total of 95 full papers presented in these proceedings was carefully reviewed and selected from 341 submissions. The papers were

organized in topical sections as follows: Part I: Best paper awards; public-key cryptanalysis; symmetric key cryptanalysis; quantum security; Part II: physical attacks, leakage and countermeasures; multiparty computation; enhanced public-key encryption and time-lock puzzles; real-world protocols; Part III: NIZK and SNARKs; theory; symmetric-key constructions; homomorphic encryption and encrypted search; Part IV: Lattice cryptanalysis; post-quantum cryptography; advanced encryption and signatures; zero-knowledge proofs, threshold and multi-signatures; authenticated key exchange. This book constitutes revised selected papers from the 22nd International Conference on Information Security and Cryptology, ICISC 2019, held in Seoul, South Korea, in December 2019. The total of 18 papers presented in this volume were carefully reviewed and selected from 43 submissions. The papers were organized in topical sections named: public-key encryption and implementation; homomorphic encryption; secure multiparty computation; post-quantum cryptography; secret sharing and searchable encryption; storage security and information retrieval; and attacks and software security. This book comprehensively reviews searchable encryption, which represents a series of research developments that directly enable search functionality over encrypted data. The book majorly covers: 1) the design and implementation of encrypted search algorithms, data structures, and systems that facilitate various forms of search over always-encrypted databases; 2) different threat models, assumptions, and the related security guarantees, when using searchable encryption in the real-world settings; and 3) latest efforts in building full-fledged encrypted database systems that draw insights from searchable encryption constructions. The book fits in the timely context, where the necessity of safeguarding important and sensitive data has been globally recognized. Traditional security measures, such as storing data behind network firewalls and layers of access control mechanisms to keep attackers out, are no longer sufficient to cope with the expanding landscape of surging cyber threats. There is an urgent call to keep sensitive data always encrypted to protect the data at rest, in transit, and in use. Doing so guarantees data confidentiality for owners, even if the data is out of their hands, e.g., hosted at in-the-cloud databases. The daunting challenge is how to perform computation over encrypted data. As we unfold in this book, searchable encryption, as a specific line of research in this broadly defined area, has received tremendous advancements over the past decades. This book is majorly oriented toward senior undergraduates, graduate students, and researchers, who want to work in the field and need

extensive coverage of encrypted database research. It also targets security practitioners who want to make well-informed deployment choices of the latest advancements in searchable encryption for their targeted applications. Hopefully, this book will be beneficial in both regards. This book constitutes the refereed proceedings of the 25th Australasian Conference on Information Security and Privacy, ACISP 2020, held in Perth, WA, Australia, in November 2020*. The 31 revised full papers and 5 short papers presented were carefully revised and selected from 151 submissions. The papers present and discuss the latest research, trends, breakthroughs, and challenges in the domain of information security, privacy and cybersecurity on a variety of topics such as post-quantum cryptography; symmetric cipher; signature; network security and blockchain; cryptographic primitives; mathematical foundation; machine learning security, among others. *The conference was held virtually due to COVID-19 pandemic. A complete, accessible book on single and multiple output Boolean functions in cryptography and coding, with recent applications and problems. This book constitutes the refereed proceedings of the 17th International Conference on Cryptology and Network Security, CANS 2018, held in Naples, Italy, in September/October 2018. The 26 full papers were carefully reviewed and selected from 79 submissions. The papers are organized in the following topical sections: privacy; Internet misbehavior and protection; malware; symmetric key cryptography; signatures; cryptanalysis; cryptographic primitives; and cryptographic protocols. This book is the most comprehensive and integrated treatment of the protocols required for authentication and key establishment. In a clear, uniform presentation the authors classify most protocols in terms of their properties and resource requirements, and describe all the main attack types, so the reader can quickly evaluate protocols for particular applications. In this edition the authors introduced new chapters and updated the text throughout in response to new developments and updated standards. The first chapter, an introduction to authentication and key establishment, provides the necessary background on cryptography, attack scenarios, and protocol goals. A new chapter, computational security models, describes computational models for key exchange and authentication and will help readers understand what a computational proof provides and how to compare the different computational models in use. In the subsequent chapters the authors explain protocols that use shared key cryptography, authentication and key transport using public key cryptography, key agreement protocols, the Transport Layer Security protocol, identity-based key agreement, password-based protocols,

and group key establishment. The book is a suitable graduate-level introduction, and a reference and overview for researchers and practitioners with 225 concrete protocols described. In the appendices the authors list and summarize the relevant standards, linking them to the main book text when appropriate, and they offer a short tutorial on how to build a key establishment protocol. The book also includes a list of protocols, a list of attacks, a summary of the notation used in the book, general and protocol indexes, and an extensive bibliography. This book constitutes selected papers from the 24th International Conference on Information Security and Cryptology, ICISC 2021, held in Seoul, South Korea, in December 2021. The total of 23 papers presented in this volume were carefully reviewed and selected from 63 submissions. The papers are arranged by topic: Cryptographic Protocol in Quantum Computer Age; Security Analysis of Hash Algorithm; Security analysis of Symmetric Key Encryption Algorithm; Fault and Side-Channel Attack; Constructions and Designs; Quantum Circuit; Efficient Implementation. The aim of this conference was to provide an international forum for the latest results of research, development, and applications within the field of information security and cryptology. This book gathers the proceedings of the Sixth International Conference on Computational Science and Technology 2019 (ICCST2019), held in Kota Kinabalu, Malaysia, on 29–30 August 2019. The respective contributions offer practitioners and researchers a range of new computational techniques and solutions, identify emerging issues, and outline future research directions, while also showing them how to apply the latest large-scale, high-performance computational methods. The Internet of Things is a technological revolution that represents the future of computing and communications. Even though efforts have been made to standardize Internet of Things devices and how they communicate with the web, a uniform architecture is not followed. This inconsistency directly impacts and limits security standards that need to be put in place to secure the data being exchanged across networks. Cryptographic Security Solutions for the Internet of Things is an essential reference source that discusses novel designs and recent developments in cryptographic security control procedures to improve the efficiency of existing security mechanisms that can help in securing sensors, devices, networks, communication, and data in the Internet of Things. With discussions on cryptographic algorithms, encryption techniques, and authentication procedures, this book is ideally designed for managers, IT consultants, startup companies, ICT procurement managers, systems and

network integrators, infrastructure service providers, students, researchers, and academic professionals. This book constitutes revised selected papers from the 19th International Conference on Information Security and Cryptology, ICISC 2016, held in Seoul, South Korea, in November/December 2016. The 18 full papers presented in this volume were carefully reviewed and selected from 69 submissions. There were organized in topical sections named: protocols; lattice cryptography; encryption; implementation and algorithms; signatures and protocol; and analysis. The three volume-set LNCS 11476, 11477, and 11478 constitute the thoroughly refereed proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2019,held in Darmstadt, Germany, in May 2019. The 76 full papers presented were carefully reviewed and selected from 327 submissions. The papers are organized into the following topical sections: ABE and CCA security; succinct arguments and secure messaging; obfuscation; block ciphers; differential privacy; bounds for symmetric cryptography; non-malleability; blockchain and consensus; homomorphic primitives; standards; searchable encryption and ORAM; proofs of work and space; secure computation; quantum, secure computation and NIZK, lattice-based cryptography; foundations; efficient secure computation; signatures; information-theoretic cryptography; and cryptanalysis. This book constitutes the proceedings of the 6th International Conference on Cryptology and Security in Latin America, LATINCRYPT 2019, held in Santiago di Chile, Chile, in October 2019. The 18 revised full papers presented were carefully reviewed and selected from 40 submissions. The papers are organized in topical sections on cryptoanalysis, symmetric cryptography, ide-channel cryptography, post-quantum cryptography, signatures and protocols, and implementation. This book constitutes the post-conference proceedings of the 15th International Conference on Information Security and Cryptology, Inscrypt 2019, held in Nanjing, China, in December 2019. The 23 full papers presented together with 8 short papers and 2 invited papers were carefully reviewed and selected from 94 submissions. The papers cover topics in the fields of post-quantum cryptology; AI security; systems security; side channel attacks; identity-based cryptography; signatures; cryptanalysis; authentication; and mathematical foundations. This book constitutes the refereed proceedings of the 20th International Conference on Cryptology in India, INDOCRYPT 2019, held in Hyderabad, India, in December 2019. The 28 revised full papers presented in this book were carefully reviewed and selected from 110 submissions (of

which 20 were either rejected without being reviewed or withdrawn before the deadline). The focus of the conference includes works on signatures and filter permutators; symmetric key ciphers and hash functions; blockchain, secure computation and blind coupon mechanism; oblivious transfer, obfuscation and privacy amplification; Boolean functions, elliptic curves and lattices; algorithms, attacks and distribution; and efficiency, side-channel resistance and PUFs. An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements. This book contains revised selected papers from the 26th International Conference on Selected Areas in Cryptography, SAC 2019, held in Waterloo, ON, Canada, in August 2019. The 26 full papers presented in this volume were carefully reviewed and selected from 74 submissions. They cover the following research areas: Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, and authenticated encryption schemes, efficient implementations of symmetric and public key algorithms, mathematical and algorithmic aspects of applied cryptology, cryptography for the Internet of Things. The

three-volume set, LNCS 11692, LNCS 11693, and LNCS 11694, constitutes the refereed proceedings of the 39th Annual International Cryptology Conference, CRYPTO 2019, held in Santa Barbara, CA, USA, in August 2019. The 81 revised full papers presented were carefully reviewed and selected from 378 submissions. The papers are organized in the following topical sections: Part I: Award papers; lattice-based ZK; symmetric cryptography; mathematical cryptanalysis; proofs of storage; non-malleable codes; SNARKs and blockchains; homomorphic cryptography; leakage models and key reuse. Part II: MPC communication complexity; symmetric cryptanalysis; (post) quantum cryptography; leakage resilience; memory hard functions and privacy amplification; attribute based encryption; foundations. Part III: Trapdoor functions; zero knowledge I; signatures and messaging; obfuscation; watermarking; secure computation; various topics; zero knowledge II; key exchange and broadcast encryption. An up-to-date guide to an overview of authentication in the Internet of Things (IoT) The Internet of things (IoT) is the network of the countless physical devices that have the possibility to connect and exchange data. Among the various security requirements, authentication to the IoT is the first step to prevent the impact of attackers. IoT Security offers an important guide into the development of the many authentication mechanisms that provide IoT authentication at various levels such as user level, device level and network level. The book covers a wide range of topics including an overview of IoT and addresses in detail the security challenges at every layer by considering both the technologies and the architecture used. The authors—noted experts on the topic—provide solutions for remediation of compromised security, as well as methods for risk mitigation, and offer suggestions for prevention and improvement. In addition, IoT Security offers a variety of illustrative use cases. This important book: Offers an authoritative reference designed for use by all IoT stakeholders Includes information for securing devices at the user, device, and network levels Contains a classification of existing vulnerabilities Written by an international group of experts on the topic Provides a guide to the most current information available on IoT security Written for network operators, cloud operators, IoT device manufacturers, IoT device users, wireless users, IoT standardization organizations, and security solution developers, IoT Security is an essential guide that contains information on security features, including underlying networks, architectures, and security requirements. The three volume-set LNCS 12105, 12106, and 12107 constitute the thoroughly refereed proceedings of the 39th Annual

International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2020, which was due to be held in Zagreb, Croatia, in May 2020. The conference was held virtually due to the COVID-19 pandemic. The 81 full papers presented were carefully reviewed and selected from 375 submissions. The papers are organized into the following topical sections: invited talk; best paper awards; obfuscation and functional encryption; symmetric cryptanalysis; randomness extraction; symmetric cryptography I; secret sharing; fault-attack security; succinct proofs; generic models; secure computation I; quantum I; foundations; isogeny-based cryptography; lattice-based cryptography; symmetric cryptography II; secure computation II; asymmetric cryptanalysis; verifiable delay functions; signatures; attribute-based encryption; side-channel security; non-interactive zero-knowledge; public-key encryption; zero-knowledge; quantum II. This book examines innovation in the fields of computer engineering and networking, and explores important, state-of-the-art developments in areas such as artificial intelligence, machine learning, information analysis and communication. It gathers papers presented at the 8th International Conference on Computer Engineering and Networks (CENet2018), held in Shanghai, China on August 17–19, 2018. • Explores emerging topics in computer engineering and networking, along with their applications • Discusses how to improve productivity by using the latest advanced technologies • Examines innovation in the fields of computer engineering and networking This book constitutes the refereed proceedings of the 19th International Conference on Information and Communications Security, ICICS 2017, held in Beijing, China, in December 2017. The 43 revised full papers and 14 short papers presented were carefully selected from 188 submissions. The papers cover topics such as Formal Analysis and Randomness Test; Signature Scheme and Key Management; Algorithms; Applied Cryptography; Attacks and Attacks Defense; Wireless Sensor Network Security; Security Applications; Malicious Code Defense and Mobile Security; IoT Security; Healthcare and Industrial Control System Security; Privacy Protection; Engineering Issues of Crypto; Cloud and E-commerce Security; Security Protocols; Network Security. The three volumes LNCS 10820, 10821, and 10822 constitute the thoroughly refereed proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2018, held in Tel Aviv, Israel, in April/May 2018. The 69 full papers presented were carefully reviewed and selected from 294 submissions. The papers are organized into

the following topical sections: foundations; lattices; random oracle model; fully homomorphic encryption; permutations; galois counter mode; attribute-based encryption; secret sharing; blockchain; multi-collision resistance; signatures; private simultaneous messages; masking; theoretical multiparty computation; obfuscation; symmetric cryptanalysis; zero-knowledge; implementing multiparty computation; non-interactive zero-knowledge; anonymous communication; isogeny; leakage; key exchange; quantum; non-malleable codes; and provable symmetric cyptography. Cryptography lies at the heart of most technologies deployed today for secure communications. At the same time, mathematics lies at the heart of cryptography, as cryptographic constructions are based on algebraic scenarios ruled by group or number theoretical laws. Understanding the involved algebraic structures is, thus, essential to design robust cryptographic schemes. This Special Issue is concerned with the interplay between group theory, symmetry and cryptography. The book highlights four exciting areas of research in which these fields intertwine: post-quantum cryptography, coding theory, computational group theory and symmetric cryptography. The articles presented demonstrate the relevance of rigorously analyzing the computational hardness of the mathematical problems used as a base for cryptographic constructions. For instance, decoding problems related to algebraic codes and rewriting problems in non-abelian groups are explored with cryptographic applications in mind. New results on the algebraic properties or symmetric cryptographic tools are also presented, moving ahead in the understanding of their security properties. In addition, post-quantum constructions for digital signatures and key exchange are explored in this Special Issue, exemplifying how (and how not) group theory may be used for developing robust cryptographic tools to withstand quantum attacks. This book constitutes the refereed proceedings of the 15th International Conference on Provable Security, ProvSec 2021, held in Guangzhou, China, in November 2021. The 21 full papers presented were carefully reviewed and selected from 67 submissions. The papers focus on provable security as an essential tool for analyzing security of modern cryptographic primitives. They are divided in the following topical sections: Searchable Encryption, Key Exchange & Zero Knowledge Proof, Post Quantum Cryptography, Functional Encryption, Digital Signature, and Practical Security Protocols. This book constitutes the refereed proceedings of the 14th International Joint Conference on E-Business and Telecommunications, ICETE 2017, held in Madrid, Spain, in July 2017. ICETE is a joint international conference

integrating four major areas of knowledge that are divided into six corresponding conferences: International Conference on Data Communication Networking, DCNET; International Conference on E-Business, ICE-B; International Conference on Optical Communication Systems, OPTICS; International Conference on Security and Cryptography, SECRYPT; International Conference on Signal Processing and Multimedia, SIGMAP; International Conference on Wireless Information Systems, WINSYS. The 17 full papers presented were carefully reviewed and selected from 195 submissions. The papers cover the following key areas of information and communication technologies, including data communication and networking, e-business and telecommunications: data communication networking; e-business; optical communication systems; security and cryptography; signal processing and multimedia applications; wireless networks and mobile systems.