

## Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

This book constitutes the refereed proceedings of the 11th International Conference on Applied Cryptography and Network Security, ACNS 2013, held in Banff, Canada, in June 2013. The 33 revised full papers included in this volume were carefully reviewed and selected from 192 submissions. They are organized in topical sections on Cloud Cryptography; Secure Computation; Hash Function and Block Cipher; Signature; System Attack; Secure Implementation - Hardware; Secure Implementation - Software; Group-oriented Systems; Key Exchange and Leakage Resilience; Cryptographic Proof; Cryptosystems.

This book constitutes the refereed proceedings of the 16th International Conference on Applied Cryptography and Network Security, ACNS 2018, held in Leuven, Belgium, in July 2018. The 36 revised full papers presented were carefully reviewed and selected from 173 submissions. The papers were organized in topical sections named: Cryptographic Protocols; Side Channel Attacks and Tamper Resistance; Digital Signatures; Privacy Preserving Computation; Multi-party Computation; Symmetric Key Primitives; Symmetric Key Cryptanalysis; Public Key Encryption; Authentication and Biometrics; Cloud and Peer-to-peer Security.

This book constitutes the proceedings of the satellite workshops held around the 18th International Conference on Applied Cryptography and Network Security, ACNS 2020, in Rome, Italy, in October 2020. The 31 papers presented in this volume were carefully reviewed and selected from 65 submissions. They stem from the following workshops: AIBlock 2020: Second International Workshop on Application Intelligence and Blockchain Security AIHWS 2020: First International Workshop on Artificial Intelligence in Hardware Security AIoTS 2020: Second International Workshop on Artificial Intelligence and Industrial Internet-of-Things Security Cloud S&P 2020: Second International Workshop on Cloud Security and Privacy SCI 2020: First International Workshop on Secure Cryptographic Implementation SecMT 2020: First International Workshop on Security in Mobile Technologies SiMLA 2020: Second International Workshop on Security in Machine Learning and its Applications

Now the most used textbook for introductory cryptography courses in both mathematics and computer science, the Third Edition builds upon previous editions by offering several new sections, topics, and exercises. The authors present the core principles of modern cryptography, with emphasis on formal definitions, rigorous proofs of security.

Cryptography will continue to play important roles in developing of new security solutions which will be in great demand with the advent of high-speed next-generation communication systems and networks. This book discusses some of the critical security challenges faced by today's computing world and provides insights to possible mechanisms to defend against these attacks. The book contains sixteen chapters which deal with security and privacy issues in computing and communication networks, quantum cryptography and the evolutionary concepts of cryptography and their applications like chaos-based cryptography and DNA

## Get Free Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

cryptography. It will be useful for researchers, engineers, graduate and doctoral students working in cryptography and security related areas. It will also be useful for faculty members of graduate schools and universities.

This book constitutes the refereed proceedings of the 4th International Conference on Applied Cryptography and Network Security, ACNS 2006, held in Singapore in June 2006. Book presents 33 revised full papers, organized in topical sections on intrusion detection and avoidance, cryptographic applications, DoS attacks and countermeasures, key management, cryptanalysis, security of limited devices, cryptography, authentication and Web security, ad-hoc and sensor network security, cryptographic constructions, and security and privacy.

This book constitutes the refereed proceedings of the 5th International Conference on Applied Cryptography and Network Security, ACNS 2007, held in Zhuhai, China, June 2007. The 31 revised full papers cover signature schemes, computer and network security, cryptanalysis, group-oriented security, cryptographic protocols, anonymous authentication, identity-based cryptography, and security in wireless, ad-hoc, and peer-to-peer networks.

This book constitutes the proceedings of the satellite workshops held around the 17th International Conference on Applied Cryptography and Network Security, ACNS 2019, in Bogota, Colombia, in June 2019. The 10 papers presented in this volume were carefully reviewed and selected from 30 submissions. They stem from the following workshops: AIBlock 2019: First International Workshop on Application Intelligence and Blockchain Security AIoT 2019: First International Workshop on Artificial Intelligence and Industrial Internet-of-Things Security Cloud S&P 2019: First International Workshop on Cloud Security and Privacy PriDA 2019: First International Workshop on Privacy-preserving Distributed Data Analysis SiMLA 2019: First International Workshop on Security in Machine Learning and its Applications

This text provides a practical survey of both the principles and practice of cryptography and network security. First, the basic issues to be addressed by a network security capability are explored through a tutorial and survey of cryptography and network security technology. Then, the practice of network security is explored via practical applications that have been implemented and are in use today.

This book constitutes the proceedings of the satellite workshops held around the 19th International Conference on Applied Cryptography and Network Security, ACNS 2021, held in Kamakura, Japan, in June 2021. The 26 papers presented in this volume were carefully reviewed and selected from 49 submissions. They stem from the following workshops: AIBlock 2021: Third International Workshop on Application Intelligence and Blockchain Security AIHWS 2021: Second International Workshop on Artificial Intelligence in Hardware Security AIoT 2021: Third International Workshop on Artificial Intelligence and Industrial IoT Security CIMSS 2021: First International Workshop on Critical Infrastructure and Manufacturing System Security Cloud S&P 2021: Third International Workshop on Cloud Security and Privacy SCI 2021: Second International Workshop on Secure Cryptographic Implementation SecMT 2021: Second International Workshop on Security in Mobile Technologies SiMLA 2021; Third International Workshop on Security in Machine Learning and its Applications Due to the Corona pandemic the workshop was held as a virtual event.

This book constitutes the refereed proceedings of the 14th International Conference on Applied Cryptography and Network Security, ACNS 2016, held in Guildford, UK, in June 2016. The 35 revised full papers included in this volume and presented together with 2 invited talks,

## Get Free Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

were carefully reviewed and selected from 183 submissions. ACNS is an annual conference focusing on innovative research and current developments that advance the areas of applied cryptography, cyber security and privacy.

The two-volume set of LNCS 12146 and 12147 constitutes the refereed proceedings of the 18th International Conference on Applied Cryptography and Network Security, ACNS 2020, held in Rome, Italy, in October 2020. The conference was held virtually due to the COVID-19 pandemic. The 46 revised full papers presented were carefully reviewed and selected from 214 submissions. The papers were organized in topical sections named: cryptographic protocols cryptographic primitives, attacks on cryptographic primitives, encryption and signature, blockchain and cryptocurrency, secure multi-party computation, post-quantum cryptography.

This book constitutes the refereed proceedings of the 9th International Conference on Applied Cryptography and Network Security, ACNS 2011, held in Nerja, Spain, in June 2011. The 31 revised full papers included in this volume were carefully reviewed and selected from 172 submissions. They are organized in topical sessions on malware and intrusion detection; attacks, applied crypto; signatures and friends; eclectic assortment; theory; encryption; broadcast encryption; and security services.

The two-volume set LNCS 12726 + 12727 constitutes the proceedings of the 19th International Conference on Applied Cryptography and Network Security, ACNS 2021, which took place virtually during June 21-24, 2021. The 37 full papers presented in the proceedings were carefully reviewed and selected from a total of 186 submissions. They were organized in topical sections as follows: Part I: Cryptographic protocols; secure and fair protocols; cryptocurrency and smart contracts; digital signatures; embedded system security; lattice cryptography; Part II: Analysis of applied systems; secure computations; cryptanalysis; system security; and cryptography and its applications.

Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering applies the principles of cryptographic systems to real-world scenarios, explaining how cryptography can protect businesses' information and ensure privacy for their networks and databases. It delves into the specific security requirements within various emerging application areas and discusses procedures for engineering cryptography into system design and implementation.

As a cybersecurity professional, discover how to implement cryptographic techniques to help your organization mitigate the risks of altered, disclosed, or stolen data Key Features Discover how cryptography is used to secure data in motion as well as at rest Compare symmetric with asymmetric encryption and learn how a hash is used Get to grips with different types of cryptographic solutions along with common applications Book Description In today's world, it is important to have confidence in your data storage and transmission strategy.

Cryptography can provide you with this confidentiality, integrity, authentication, and non-repudiation. But are you aware of just what exactly is involved in using cryptographic techniques? Modern Cryptography for Cybersecurity Professionals helps you to gain a better understanding of the cryptographic elements necessary to secure your data. The book begins by helping you to understand why we need to secure data and how encryption can provide protection, whether it be in motion or at rest. You'll then delve into symmetric and asymmetric encryption and discover how a hash is used. As you advance, you'll see how the public key infrastructure (PKI) and certificates build trust between parties, so that we can confidently encrypt and exchange data. Finally, you'll explore the practical applications of cryptographic techniques, including passwords, email, and blockchain technology, along with securely transmitting data using a virtual private network (VPN). By the end of this cryptography book, you'll have gained a solid understanding of cryptographic techniques and terms, learned how symmetric and asymmetric encryption and hashed are used, and recognized the importance of key management and the PKI. What you will learn Understand how network attacks can compromise data Review practical uses of cryptography over time Compare how symmetric and asymmetric encryption

## Get Free Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

work Explore how a hash can ensure data integrity and authentication Understand the laws that govern the need to secure data Discover the practical applications of cryptographic techniques Find out how the PKI enables trust Get to grips with how data can be secured using a VPN Who this book is for This book is for IT managers, security professionals, students, teachers, and anyone looking to learn more about cryptography and understand why it is important in an organization as part of an overall security framework. A basic understanding of encryption and general networking terms and concepts is needed to get the most out of this book.

This book constitutes the refereed proceedings of the 10th International Conference on Applied Cryptography and Network Security, ACNS 2012, held in Singapore, in June 2012. The 33 revised full papers included in this volume were carefully reviewed and selected from 192 submissions. They are organized in topical sessions on authentication, key management, block ciphers, identity-based cryptography, cryptographic primitives, cryptanalysis, side channel attacks, network security, Web security, security and privacy in social networks, security and privacy in RFID systems, security and privacy in cloud systems, and security and privacy in smart grids.

Cryptography, in particular public-key cryptography, has emerged in the last 20 years as an important discipline that is not only the subject of an enormous amount of research, but provides the foundation for information security in many applications. Standards are emerging to meet the demands for cryptographic protection in most areas of data communications. Public-key cryptographic techniques are now in widespread use, especially in the financial services industry, in the public sector, and by individuals for their personal privacy, such as in electronic mail. This Handbook will serve as a valuable reference for the novice as well as for the expert who needs a wider scope of coverage within the area of cryptography. It is a necessary and timely guide for professionals who practice the art of cryptography. The Handbook of Applied Cryptography provides a treatment that is multifunctional: It serves as an introduction to the more practical aspects of both conventional and public-key cryptography It is a valuable source of the latest techniques and algorithms for the serious practitioner It provides an integrated treatment of the field, while still presenting each major topic as a self-contained unit It provides a mathematical treatment to accompany practical discussions It contains enough abstraction to be a valuable reference for theoreticians while containing enough detail to actually allow implementation of the algorithms discussed Now in its third printing, this is the definitive cryptography reference that the novice as well as experienced developers, designers, researchers, engineers, computer scientists, and mathematicians alike will use.

"This special Anniversary Edition celebrates 20 years for the most definitive reference on cryptography ever published." -- Book jacket. New introduction by the author.

From the world's most renowned security technologist, Bruce Schneier, this 20th Anniversary Edition is the most definitive reference on cryptography ever published and is the seminal work on cryptography. Cryptographic techniques have applications far beyond the obvious uses of encoding and decoding information. For developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there's no better overview than Applied Cryptography, the definitive book on the subject. Bruce Schneier covers general classes of cryptographic protocols and then specific techniques, detailing the

## Get Free Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

inner workings of real-world cryptographic algorithms including the Data Encryption Standard and RSA public-key cryptosystems. The book includes source-code listings and extensive advice on the practical aspects of cryptography implementation, such as the importance of generating truly random numbers and of keeping keys secure. ". . .the best introduction to cryptography I've ever seen. . . .The book the National Security Agency wanted never to be published. . . ." -Wired Magazine ". . .monumental . . . fascinating . . . comprehensive . . . the definitive work on cryptography for computer programmers . . ." -Dr. Dobb's Journal ". . .easily ranks as one of the most authoritative in its field." -PC Magazine The book details how programmers and electronic communications professionals can use cryptography-the technique of enciphering and deciphering messages-to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems. The book shows programmers who design computer applications, networks, and storage systems how they can build security into their software and systems. With a new Introduction by the author, this premium edition will be a keepsake for all those committed to computer and cyber security. This book constitutes the refereed proceedings of the 13th International Conference on Applied Cryptography and Network Security, ACNS 2015, held in New York, NY, USA, in June 2015. The 33 revised full papers included in this volume and presented together with 2 abstracts of invited talks, were carefully reviewed and selected from 157 submissions. They are organized in topical sections on secure computation: primitives and new models; public key cryptographic primitives; secure computation II: applications; anonymity and related applications; cryptanalysis and attacks (symmetric crypto); privacy and policy enforcement; authentication via eye tracking and proofs of proximity; malware analysis and side channel attacks; side channel countermeasures and tamper resistance/PUFs; and leakage resilience and pseudorandomness.

Cryptography is now ubiquitous – moving beyond the traditional environments, such as government communications and banking systems, we see cryptographic techniques realized in Web browsers, e-mail programs, cell phones, manufacturing systems, embedded software, smart buildings, cars, and even medical implants. Today's designers need a comprehensive understanding of applied cryptography. After an introduction to cryptography and data security, the authors explain the main techniques in modern cryptography, with chapters addressing stream ciphers, the Data Encryption Standard (DES) and 3DES, the Advanced Encryption Standard (AES), block ciphers, the RSA cryptosystem, public-key cryptosystems based on the discrete logarithm problem, elliptic-curve cryptography (ECC), digital signatures, hash functions, Message Authentication Codes (MACs), and methods for key establishment, including certificates and public-key infrastructure (PKI). Throughout the book, the authors focus on communicating the essentials and keeping the mathematics to a minimum, and they move quickly from explaining the foundations to describing practical implementations, including recent topics such as lightweight ciphers for RFIDs and mobile devices, and current key-length recommendations. The authors have considerable experience teaching applied cryptography to engineering and computer science students and to professionals, and they make extensive use of examples, problems, and chapter reviews, while the book's website offers slides, projects and links to further resources. This is a suitable textbook for graduate and advanced



## Get Free Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

undergraduate courses and also for self-study by engineers.

This book constitutes the proceedings of the 15th International Conference on Applied Cryptology and Network Security, ACNS 2017, held in Kanazawa, Japan, in July 2017. The 34 papers presented in this volume were carefully reviewed and selected from 149 submissions. The topics focus on innovative research and current developments that advance the areas of applied cryptography, security analysis, cyber security and privacy, data and server security.

This book constitutes the refereed proceedings of the 6th International Conference on Applied Cryptography and Network Security, ACNS 2008, held in New York, NY, USA, in June 2008. The 30 revised full papers presented were carefully reviewed and selected from 131 submissions. The papers address all aspects of applied cryptography and network security with special focus on novel paradigms, original directions, and non-traditional perspectives.

Information Systems (IS) are a nearly omnipresent aspect of the modern world, playing crucial roles in the fields of science and engineering, business and law, art and culture, politics and government, and many others. As such, identity theft and unauthorized access to these systems are serious concerns. *Theory and Practice of Cryptography Solutions for Secure Information Systems* explores current trends in IS security technologies, techniques, and concerns, primarily through the use of cryptographic tools to safeguard valuable information resources. This reference book serves the needs of professionals, academics, and students requiring dedicated information systems free from outside interference, as well as developers of secure IS applications. This book is part of the *Advances in Information Security, Privacy, and Ethics* series collection.

The Department of Electrical Engineering-ESAT at the Katholieke Universiteit Leuven regularly runs a course on the state of the art and evolution of computer security and industrial cryptography. The first course took place in 1983, the second in 1989, and since then the course has been a biennial event. The course is intended for both researchers and practitioners from industry and government. It covers the basic principles as well as the most recent developments. Our own interests mean that the course emphasizes cryptography, but we also ensure that the most important topics in computer security are covered. We try to strike a good balance between basic theory and real-life applications, between mathematical background and judicial aspects, and between recent technical developments and standardization issues. Perhaps the greatest strength of the course is the creation of an environment that enables dialogue between people from diverse professions and backgrounds. In 1993, we published the formal proceedings of the course in the *Lecture Notes in Computer Science* series (Volume 741). Since the field of cryptography has advanced considerably during the interim period, there is a clear need to publish a new edition. Since 1993, several excellent textbooks and handbooks on cryptology have been published and the need for introductory-level papers has decreased. The growth of the main

## Get Free Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

conferences in cryptology (Eurocrypt, Crypto, and Asiacrypt) shows that interest in the field is increasing. An all-practical guide to the cryptography behind common tools and protocols that will help you make excellent security choices for your systems and applications. In *Real-World Cryptography*, you will find:

- Best practices for using cryptography
- Diagrams and explanations of cryptographic algorithms
- Implementing digital signatures and zero-knowledge proofs
- Specialized hardware for attacks and highly adversarial environments
- Identifying and fixing bad practices
- Choosing the right cryptographic tool for any problem

*Real-World Cryptography* reveals the cryptographic techniques that drive the security of web APIs, registering and logging in users, and even the blockchain. You'll learn how these techniques power modern security, and how to apply them to your own projects. Alongside modern methods, the book also anticipates the future of cryptography, diving into emerging and cutting-edge advances such as cryptocurrencies, and post-quantum cryptography. All techniques are fully illustrated with diagrams and examples so you can easily see how to put them into practice. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications.

About the technology Cryptography is the essential foundation of IT security. To stay ahead of the bad actors attacking your systems, you need to understand the tools, frameworks, and protocols that protect your networks and applications. This book introduces authentication, encryption, signatures, secret-keeping, and other cryptography concepts in plain language and beautiful illustrations.

About the book *Real-World Cryptography* teaches practical techniques for day-to-day work as a developer, sysadmin, or security practitioner. There's no complex math or jargon: Modern cryptography methods are explored through clever graphics and real-world use cases. You'll learn building blocks like hash functions and signatures; cryptographic protocols like HTTPS and secure messaging; and cutting-edge advances like post-quantum cryptography and cryptocurrencies. This book is a joy to read—and it might just save your bacon the next time you're targeted by an adversary after your data.

What's inside

- Implementing digital signatures and zero-knowledge proofs
- Specialized hardware for attacks and highly adversarial environments
- Identifying and fixing bad practices
- Choosing the right cryptographic tool for any problem

About the reader For cryptography beginners with no previous experience in the field.

About the author David Wong is a cryptography engineer. He is an active contributor to internet standards including Transport Layer Security.

Table of Contents

PART 1 PRIMITIVES: THE INGREDIENTS OF CRYPTOGRAPHY

- 1 Introduction
- 2 Hash functions
- 3 Message authentication codes
- 4 Authenticated encryption
- 5 Key exchanges
- 6 Asymmetric encryption and hybrid encryption
- 7 Signatures and zero-knowledge proofs
- 8 Randomness and secrets

PART 2 PROTOCOLS: THE RECIPES OF CRYPTOGRAPHY

- 9 Secure transport
- 10 End-to-end encryption
- 11 User authentication
- 12 Crypto as in cryptocurrency?
- 13 Hardware cryptography
- 14 Post-quantum cryptography
- 15 Is this it? Next-generation cryptography
- 16 When and where cryptography fails

## Get Free Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

This book constitutes the refereed proceedings of the 7th International Conference on Applied Cryptography and Network Security, ACNS 2009, held in Paris-Rocquencourt, France, in June 2009. The 32 revised full papers presented were carefully reviewed and selected from 150 submissions. The papers are organized in topical sections on key exchange, secure computation, public-key encryption, network security, traitor tracing, authentication and anonymity, hash functions, lattices, and side-channel attacks.

This book constitutes the refereed proceedings of the Second International Conference on Applied Cryptography and Network Security, ACNS 2004, held in Yellow Mountain, China, in June 2004. The 36 revised full papers presented were carefully reviewed and selected from 297 submissions. The papers are organized in topical sections on security and storage, provably secure constructions, Internet security, digital signatures, security modeling, authenticated key exchange, security of deployed systems, cryptosystems design and analysis, cryptographic protocols, side channels and protocol analysis, intrusion detection and DoS, and cryptographic algorithms.

The 3rd International Conference on Applied Cryptography and Network Security (ACNS 2005) was sponsored and organized by ICISA (the International Communications and Information Security Association). It was held at Columbia University in New York, USA, June 7–10, 2005. This conference proceedings volume contains papers presented in the academic/research track. ACNS covers a large number of research areas that have been gaining importance in recent years due to the development of the Internet, wireless communication and the increased global exposure of computing resources. The papers in this volume are representative of the state of the art in security and cryptography research, worldwide. The Program Committee of the conference received a total of 158 submissions from all over the world, of which 35 submissions were selected for presentation at the academic track. In addition to this track, the conference also hosted a technical/ industrial/ short papers track whose presentations were also carefully selected from among the submissions. All submissions were reviewed by experts in the relevant areas.

This practical guide to modern encryption breaks down the fundamental mathematical concepts at the heart of cryptography without shying away from meaty discussions of how they work. You'll learn about authenticated encryption, secure randomness, hash functions, block ciphers, and public-key techniques such as RSA and elliptic curve cryptography. You'll also learn:

- Key concepts in cryptography, such as computational security, attacker models, and forward secrecy
- The strengths and limitations of the TLS protocol behind HTTPS secure websites
- Quantum computation and post-quantum cryptography
- About various vulnerabilities by examining numerous code examples and use cases
- How to choose the best algorithm or protocol and ask vendors the right questions

Each chapter includes a discussion of common implementation mistakes using real-world examples and details what could go wrong and how to



## Get Free Applied Cryptography For Cyber Security And Defense Information Encryption And Cyphering

avoid these pitfalls. Whether you're a seasoned practitioner or a beginner looking to dive into the field, *Serious Cryptography* will provide a complete survey of modern encryption and its applications.

The ultimate guide to cryptography, updated from an author team of the world's top cryptography experts. Cryptography is vital to keeping information safe, in an era when the formula to do so becomes more and more challenging. Written by a team of world-renowned cryptography experts, this essential guide is the definitive introduction to all major areas of cryptography: message security, key negotiation, and key management. You'll learn how to think like a cryptographer. You'll discover techniques for building cryptography into products from the start and you'll examine the many technical changes in the field. After a basic overview of cryptography and what it means today, this indispensable resource covers such topics as block ciphers, block modes, hash functions, encryption modes, message authentication codes, implementation issues, negotiation protocols, and more. Helpful examples and hands-on exercises enhance your understanding of the multi-faceted field of cryptography. An author team of internationally recognized cryptography experts updates you on vital topics in the field of cryptography Shows you how to build cryptography into products from the start Examines updates and changes to cryptography Includes coverage on key servers, message security, authentication codes, new standards, block ciphers, message authentication codes, and more *Cryptography Engineering* gets you up to speed in the ever-evolving field of cryptography.

Applied Cryptography and Network Security 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011, Proceedings Springer

The 1st International Conference on "Applied Cryptography and Network Security" (ACNS 2003) was sponsored and organized by ICISA (International Communications and Information Security Association), in cooperation with MiAn Pte. Ltd. and the Kunming government. It was held in Kunming, China in October 2003. The conference proceedings was published as Volume 2846 of the Lecture Notes in Computer Science (LNCS) series of Springer-Verlag. The conference received 191 submissions, from 24 countries and regions; 32 of these papers were accepted, representing 15 countries and regions (acceptance rate of 16.75%). In this volume you will find the revised versions of the accepted papers that were presented at the conference. In addition to the main track of presentations of accepted papers, an additional track was held in the conference where presentations of an industrial and technical nature were given. These presentations were also carefully selected from a large set of presentation proposals. This new international conference series is the result of the vision of Dr. Yongfei Han. The conference concentrates on current developments that advance the areas of applied cryptography and its application to systems and network security. The goal is to represent both academic research works and developments in industrial and technical frontiers. We thank Dr. Han for initiating this conference and

