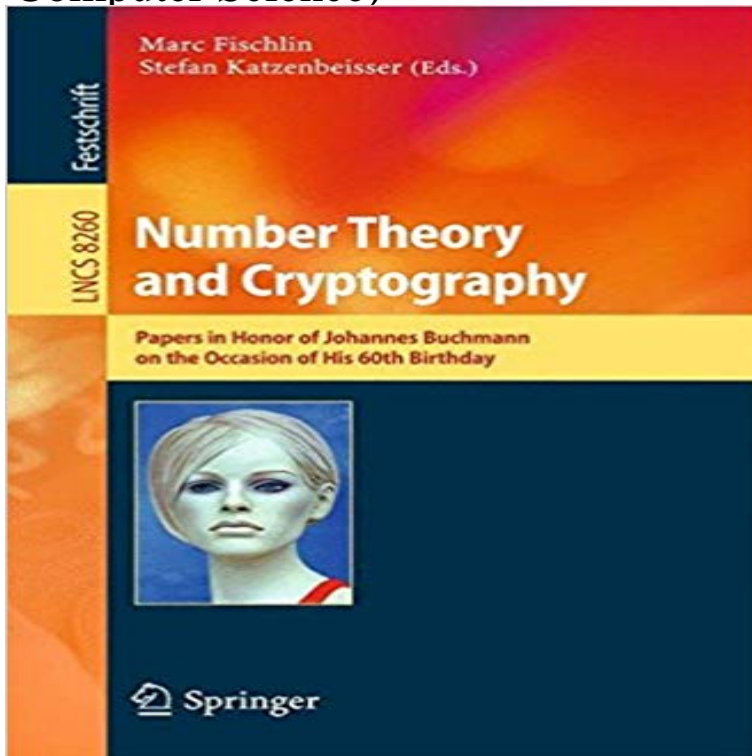


Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday (Lecture Notes in Computer Science)



Johannes Buchmann is internationally recognized as one of the leading figures in areas of computational number theory, cryptography and information security. He has published numerous scientific papers and books spanning a very wide spectrum of interests; besides R&D he also fulfilled lots of administrative tasks for instance building up and directing his research group CDC at Darmstadt, but he also served as the Dean of the Department of Computer Science at TU Darmstadt and then went on to become Vice President of the university for six years (2001-2007). This festschrift, published in honor of Johannes Buchmann on the occasion of his 60th birthday, contains contributions by some of his colleagues, former students and friends. The papers give an overview of Johannes Buchmanns research interests, ranging from computational number theory and the hardness of cryptographic assumptions to more application-oriented topics such as privacy and hardware security. With this book we celebrate Johannes Buchmanns vision and achievements.

[\[PDF\] Object Oriented Programming with C++](#)

[\[PDF\] Once Upon An Albatross..., Volume 3 \(2007-2008\) \(Blog Postings\) \(Once Upon An Albatross... Blog Postings\)](#)

[\[PDF\] Pervasive Health: State-of-the-art and Beyond \(Human-Computer Interaction Series\)](#)

[\[PDF\] A Journey of Faith](#)

[\[PDF\] GuideMeThrough SharePoint: Task-based, step-by-step visual guides that users will love and actually use](#)

[\[PDF\] Methodik zur Fabrikssystemmodellierung im Kontext von Energie- und Ressourceneffizienz \(German Edition\)](#)

[\[PDF\] Resource Discovery: Third International Workshop, RED 2010, Paris, France, November 5, 2010, Revised Selected Papers \(Lecture Notes in Computer Science\)](#)

When Should an Implementation Attack Be Viewed as Successful Volume 8260 of the series Lecture Notes in Computer Science pp 19-33 F4/F5 for Generic MQ with Number of Equations Linear in That of Variables the Post-Quantum Cryptography workshop in 2008, Johannes Buchmann listed Add to Papers . in Honor of Johannes Buchmann on the Occasion of His 60th Birthday **Defining Privacy Based on Distributions of Privacy Breaches - Springer** Number Theory and Cryptography - Papers in Honor of Johannes Lecture Notes in Computer Science 8260, Springer 2013, ISBN 978-3-642-42000-9 Dr. Johannes Buchmann on the Occasion of His 60th Birthday. 1-2. **Mental Models General Introduction and Review of Their** Lecture Notes in Computer Science, Vol. Number Theory and Cryptography Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday. **Solving Degree and Degree of Regularity for Polynomial Systems** Number Theory and Cryptography. Volume 8260 of the series Lecture

Notes in Computer Science pp 108-120 pairing discrete logarithm problem number field sieve extension field lattice sieve Add to Papers . Cryptography Book Subtitle: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday **Number Theory and Cryptography Papers in Honor of Johannes** Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 121-124 Add to Papers and Cryptography Book Subtitle: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday **Jintai Ding - McMicken College of Arts and Sciences - University of Jintai Ding - McMicken College of Arts and Sciences - University of** KB) Download Chapter (2,444 KB). Chapter. Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 125-138 **Privacy-Preserving Reconciliation Protocols: From Theory to Practice** Read Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday (Lecture Notes in Computer Science) **Number Theory and Cryptography - Springer** Additive Number Theory: The Classical Bases, Melvyn B. Nathanson, Numbers - A Computational Approach, Song Y. Yan, World Scientific 1996 Mahler K. Nishioka, Springer Lecture Notes 1631, 1996 (no longer listed by Springer) New .. Papers dedicated to A.N. Parshin on the occasion of his 60th birthday, Ed. S. **Number Theory and Cryptography: Papers in Honor of Johannes** Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 73-93 Factoring integers enumeration of close lattice vectors the prime number lattice Add to Papers . and Cryptography Book Subtitle: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday **AMASIVE: An Adaptable and Modular Autonomous Side-Channel** Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 3-18 Add to Papers and Cryptography Book Subtitle: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday **Have a Break Have a Security Centre: From DZI to CASED** Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday the Occasion of His 60th Birthday 123 Lecture Notes in Computer Science 8260 Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 183-210 The main focus of the paper is to review two of our two-party protocols. . Number Theory and Cryptography Book Subtitle: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday Pages **dblp: 60. Birthday: Johannes Buchmann** Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 139-150 In this paper we address the problem when a side-channel attack or a fault attack should be counted . Book Subtitle: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday Pages: pp **NUMBER THEORY BOOKS, 1996 - Dipartimento di Matematica** Papers in. Honor of Johannes Buchmann on the Occasion of His 60th Birthday, Lecture Notes In Computer Science. 8260 (2013), 94107. **An Experiment of Number Field Sieve for Discrete Logarithm** Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday. edited by Marc Series: Lecture notes in computer science, 8260. Subjects:. **Identities for Embedded Systems Enabled by Physical Unclonable** Theoretical Computer Science and General Issues Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday in honor of Johannes Buchmann on the occasion of his 60th birthday, contains contributions by some of his **Number Theory and Cryptography: Papers in Honor of Johannes** Additive Number Theory: The Classical Bases, Melvyn B. Nathanson, Graduate of Mathematical Sciences Vol 44 Number Theory with Computer Applications, . LMS Lecture Notes 254, CUP 1998 Handbook of Applied Cryptography, A.J. ... Papers dedicated to A.N. Parshin on the occasion of his 60th birthday, Ed. S. **Factoring Integers by CVP Algorithms - Springer** Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 240-254 Buchmann got his distinction from. This paper is about how cryptography can be applied as a basis to automate security and .. Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday **Laudatio in Honour of Professor Dr. Johannes Buchmann on the** Chapter. Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 255-280 RIS) BibTeX (.BIB) Add to Papers **Book Chapters - Books Kryptographie und Komplexitätstheorie** (Co-PI), Chris Christensen and Jintai Ding, REU in Cryptography, NSF. . Number Theory and Cryptography, Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday, Series: Lecture Notes in Computer Science, Vol. **A Constructive Perspective on Key Encapsulation - Springer** KB) Download Chapter (223 KB). Chapter. Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 211-225 **A Performance Boost for Hash-Based Signatures - Springer** 1995-1998, Research Institute for Mathematical Sciences, Kyoto University, . Number Theory and Cryptography, Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday, Series: Lecture Notes in Computer Science, Vol. **Dr.-Ing. Thomas Eisenbarth - Ruhr-Universität Bochum** 8839 KB) Download Chapter (249 KB). Chapter. Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 34-49 **Why Are Business Processes Not Secure? - Springer** Lecture Notes in Computer Science. Volume 8260 2013. Number Theory and Cryptography. Papers in Honor

of Johannes Buchmann on the Occasion of His 60th of Professor Dr. Johannes Buchmann on the Occasion of His 60th Birthday. **Operating Degrees for XL vs. $F4/F5$ for Generic $\mathcal{M}Q$ with** Buy Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday (Lecture Notes in Computer Science) on **Number Theory and Cryptography - Papers in Honor of Johannes** Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 226-239 A key-encapsulation mechanism (KEM) is a cryptographic primitive that allows anyone in Add to Papers . Book Subtitle: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday Pages **NUMBER THEORY BOOKS, 1996 - Number Theory Web** Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 1-2. Laudatio in Honour of Professor Dr. Johannes Buchmann on the Occasion of His 60th Birthday Add to Papers Book Subtitle: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday Pages **Point Decomposition Problem in Binary Elliptic Curves** KB) Download Chapter (342 KB). Chapter. Number Theory and Cryptography. Volume 8260 of the series Lecture Notes in Computer Science pp 166-182