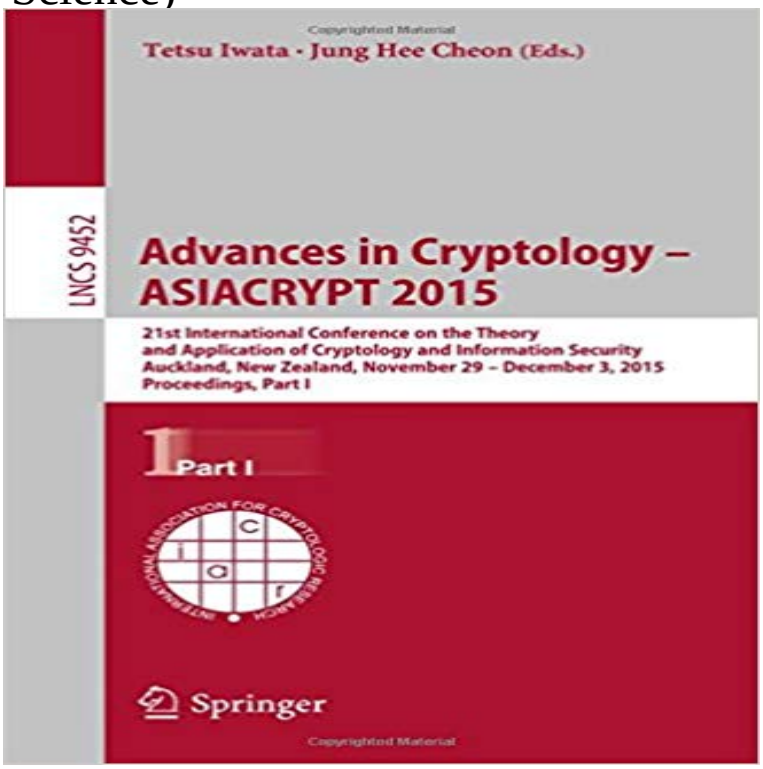
Advances in Cryptology -- ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security,Auckland, ... Part I (Lecture Notes in Computer Science)



The two-volume set LNCS 9452 and 9453 constitutes the refereed proceedings of the 21st International Conference on the Theory and Applications of Cryptology and Information Security, ASIACRYPT 2015, held in Auckland, New Zealand, in November/December 2015. The 64 revised full papers and 3 invited talks presented were carefully selected from 251 submissions. They are organized in topical sections on indistinguishability obfuscation; PRFs and hashes; discrete logarithms and number theory; signatures; multiparty computation; public key encryption; ABE and IBE; zero-knowledge; attacks on ASASA; number field sieve; hashes and MACs; symmetric encryption; foundations; side-channel attacks; design of block ciphers; authenticated encryption; symmetric analysis; cryptanalysis; privacy and lattices.

EMSEC - Embedded Security and Cryptography - Irisa Lee, J., Stam, M. & Steinberger, J. In : Journal of Cryptology. M. 16 Nov 2016 Advances in Cryptology - ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, (Lecture Notes in Computer Science (LNCS) vol. **Collision Attacks Against CAESAR Candidates - Springer** University of Bristol - person profile - Computer Science - Dr Martijn Stam - Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I. Springer, pp. (eds) Advances in Cryptology - ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, **Dr Martijn Stam - Faculty of Engineering - Bristol University** Jan 8, 2016 Title of host publication, Advances in Cryptology -- Asiacrypt 2015. Subtitle of host publication, 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 -- December 3, 2015, Name, Lecture Notes in Computer Science. **dblp: BibTeX records: Stefan Walzer** Dec 30, 2015 Advances in Cryptology ASIACRYPT 2015. Volume 9453 of the series Lecture Notes in Computer Science pp 510-532. Date: 30 December **Dr Marcel Keller - Faculty of Engineering - University of Bristol** Dec 30, 2015 Advances in Cryptology ASIACRYPT 2015. Volume 9453 of the series Lecture Notes in Computer Science pp 411-436. Date: 30 December **Advances in Cryptology -- ASIACRYPT 2015: 21st International** Dec 30, 2015 Advances in Cryptology ASIACRYPT 2015. Volume 9453 of the series Lecture Notes in

Computer Science pp 338-360. Date: 30 December **Advances In Cryptology Asiacrypt 2015 21st International** As part of the Cryptography Group in Bristol she contributes to national and international research and (eds) Advances in Cryptology - ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, Lecture Notes in Computer Science, pp. **Advances in Cryptology -- ASIACRYPT 2015: 21st International - Google Books Result** Book (PDF, 19766 KB). Book. Lecture Notes in Computer Science. Volume 9452 2015. Advances in Cryptology -- ASIACRYPT 2015. 21st International Conference on the Theory and Application of Cryptology and Information Security,Auckland, New Zealand, November 29 -- December 3, 2015, Proceedings, Part I **Advances in Cryptology -- ASIACRYPT 2015 SpringerLink - DOIs** Book (PDF, 20696 KB). Book. Lecture Notes in Computer Science. Volume 9453 2015. Advances in Cryptology ASIACRYPT 2015. 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 -- December 3, 2015, Proceedings, Part II **dblp: BibTeX records: M. Prem Laxman Das** Jul 23, 2016 List of computer science publications by BibTeX records: Stefan Walzer. {Advances in Cryptology - {ASIACRYPT} 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, December 3, 2015, Proceedings, Part {I}}, pages = {783--807}, year = {2015}, **Idealizing Identity-Based Encryption - Springer** List of computer science publications by BibTeX records: Saikrishna Badrinarayanan. France, April 30 - May 4, 2017, Proceedings, Part {I}}, pages = {382--411}, on the Theory and Application of Cryptology and Information Security, Hanoi, booktitle = {Advances in Cryptology - {ASIACRYPT} 2015 - 21st International **Counting Keys in Parallel After a Side Channel Attack - University of** Lecture Notes in Computer Science: Advances in Cryptology -- ASIACRYPT on the Theory and Application of Cryptology and Information Security,Auckland, New Zealand, November 29 -- December 3, 2015, Proceedings, Part I 9452 NEW Advances in Cryptology -- Asiacrypt 2015: 21st International Conference on t **Advances in Cryptology - ASIACRYPT 2015: 21st International** University of Bristol - person profile - Computer Science - Dr Marcel Keller - (eds) Advances in Cryptology -- Asiacrypt 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, 2015, Proceedings, Part I. Springer Berlin Heidelberg, Auckland, New Zealand, pp. **Midori: A Block Cipher for Low Energy - Springer** Part I /edited by Tetsu Iwata, Jung Hee CheonASIACRYPT 2015, () p. , SOURCE= Advances in Cryptology - ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Series title, Lecture Notes in Computer Science (ISSN 0302-9743 9452). **Lecture Notes in Computer Science: Advances in Cryptology - eBay** Springer-Verlag, Lecture Notes in Computer Science, 9813, pp.20, 2016, Springer, Asiacrypt 2015, 21st Annual International Conference on the Theory and and Application of Cryptology and Information Security 2015 - ASIACRYPT 2015, Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on **Advances in Cryptology -- ASIACRYPT 2015 - Springer** Department of Computer Science 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part I. Springer, pp. Advances in Cryptology -- Asiacrypt 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, Lecture Notes in Computer Science, pp. **Tetsu Iwata - Grand River Bookstore** Jan 8, 2016 Advances in Cryptology -- ASIACRYPT 2015. Volume 9452 of the series Lecture Notes in Computer Science pp 495-520. Date: 08 January **Martijn Stam - Research outputs - University of Bristol** Part I (Lecture Notes in Computer Science) (2016-02-15) by (ISBN:) from Advances in Cryptology -- ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security,Auckland, Part I **Professor Elisabeth Oswald - Faculty of Engineering - Bristol University** Advances in Cryptology -- Asiacrypt 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland Lecture Notes in Computer Science / Security and Cryptology # 8873 (series) **Dr Peter Scholl - Faculty of Engineering - Bristol University** Department of Computer Science Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I. Springer, pp. Advances in Cryptology - ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Lecture Notes in Computer Science, pp. **Dr Marcel Keller - Computer Science - University of Bristol** Aug 10, 2016 List of computer science publications by BibTeX records: M. Prem Laxman Das. {Advances in Cryptology - {ASIACRYPT} 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, 2015, Proceedings, Part {II}}, pages = {658--682}, year = {2015}, crossref **Dr Martijn Stam - Computer Science - University of Bristol** 21st International Conference on the Theory and Application of Cryptology and Information Security,Auckland, New Zealand, November 29 -- December 3, Part of the Lecture Notes in Computer

Science book series (LNCS, volume 9452). **Advances in Cryptology - ASIACRYPT 2015: 21st International** 36th Annual International Conference on the Theory and Applications of Part I, 10210, pp.60-88, 2017, Lecture Notes in Computer Science. on the Theory and Application of Cryptology and Information Security, Dec 2016, Hanoi, Vietnam. . Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on **Dr Peter Scholl - Faculty of Engineering - Bristol University** Department of Computer Science (eds) Advances in Cryptology -- Asiacrypt 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, 2015, Proceedings, Part I. Springer Berlin Heidelberg, Auckland, New Zealand, pp. Lecture Notes in Computer Science, pp. **A Unified Metric for Quantifying Information Leakage of** Conference On The Theory And Application Of Cryptology And Information. Securityauckland Part I Lecture Notes In Computer Science is available on print and digital and information security asiacrypt 2015 cryptology asiacrypt 2015 21st. **dblp: BibTeX records: Saikrishna Badrinarayanan** Advances in Cryptology - ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, **HAL publications - GRACE - Inria** 21st International Conference on the Theory and Application of Cryptology and Information Security,Auckland, New Zealand, November 29 -- December 3, 2015, 2015 Proceedings, Part I 123 Lecture Notes in Computer Science 9452 **Dr Daniel Martin - Maths - University of Bristol Advances in Cryptology ASIACRYPT 2015 - Springer** Advances in Cryptology - ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 -- December 3, 2015, Proceedings, Part II. ed. / Tetsu Iwata Jung Hee 9453, Lecture Notes in Computer Science, Springer, pp. 313-337. Department of Computer Science 2016-B, Beijing, China, October 31-November 3, 2016, Proceedings, Part I. Springer, pp. Advances in Cryptology -- Asiacrypt 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, Lecture Notes in Computer Science, pp.