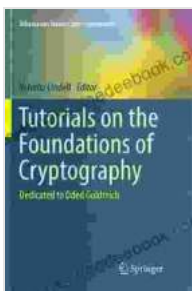


Dedicated to Oded Goldreich: Information Security and Cryptography

Oded Goldreich is a world-renowned computer scientist and cryptographer who has made significant contributions to the field of information security. He is a professor at the Weizmann Institute of Science in Israel and has been the recipient of numerous awards, including the Turing Award, the highest honor in computer science.

Early Life and Education

Oded Goldreich was born in Israel in 1953. He earned his undergraduate degree in mathematics and computer science from the Hebrew University of Jerusalem in 1976 and his Ph.D. in computer science from the Weizmann Institute of Science in 1983. His doctoral thesis, supervised by Adi Shamir, was on the complexity of proof systems.



Tutorials on the Foundations of Cryptography: Dedicated to Oded Goldreich (Information Security and Cryptography) by Yehuda Lindell

★★★★★ 5 out of 5
Language : English
File size : 10079 KB
Print length : 465 pages
Paperback : 62 pages
Item Weight : 5.1 ounces
Dimensions : 6 x 0.14 x 9 inches
Screen Reader : Supported



Research Contributions

Goldreich's research interests lie in the area of information security, with a focus on cryptography. He has made significant contributions to a wide range of topics in this field, including:

- **Foundations of cryptography:** Goldreich has developed a formal framework for cryptography that provides a rigorous foundation for the design and analysis of cryptographic protocols.
- **Pseudorandom generators:** Goldreich has developed new techniques for constructing pseudorandom generators, which are essential for many cryptographic applications.
- **Zero-knowledge proofs:** Goldreich has developed new zero-knowledge proof systems, which allow one party to prove to another party that they know a secret without revealing the secret itself.
- **Multiparty computation:** Goldreich has developed new protocols for multiparty computation, which allow multiple parties to compute a function on their inputs without revealing their inputs to each other.

Awards and Honors

Goldreich has received numerous awards and honors for his research, including:

- **Turing Award:** The Turing Award is the highest honor in computer science, and Goldreich was awarded the Turing Award in 2017 for his contributions to cryptography.
- **Gödel Prize:** The Gödel Prize is awarded annually by the Association for Computing Machinery (ACM) for outstanding papers in theoretical

computer science, and Goldreich has won the Gödel Prize three times, in 1993, 2001, and 2017.

- **RSA Award:** The RSA Award is awarded annually by RSA Security for outstanding contributions to cryptography, and Goldreich was awarded the RSA Award in 2018.

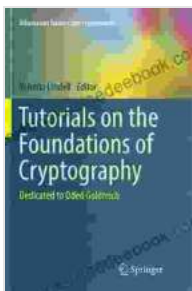
Legacy

Oded Goldreich is one of the most influential computer scientists of our time. His research has had a major impact on the field of information security, and he continues to be an active researcher and mentor to the next generation of cryptographers.

Goldreich's legacy will continue to inspire and guide future generations of computer scientists and cryptographers for years to come.

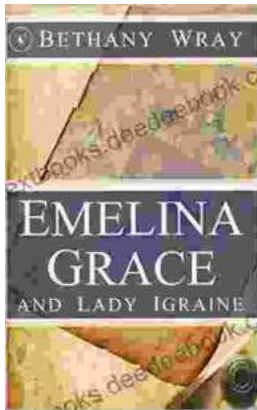
Additional Resources

- Oded Goldreich's website
- Oded Goldreich's Wikipedia page
- Oded Goldreich's Turing Award citation



Tutorials on the Foundations of Cryptography: Dedicated to Oded Goldreich (Information Security and Cryptography) by Yehuda Lindell

★ ★ ★ ★ ★ 5 out of 5
Language : English
File size : 10079 KB
Print length : 465 pages
Paperback : 62 pages
Item Weight : 5.1 ounces
Dimensions : 6 x 0.14 x 9 inches



Unveiling the Enchanting Legends of Emelina Grace and Lady Igraine: A Tale of Love, Magic, and Timelessness

Emelina Grace: The Enchanted Forest Nymph In the depths of an ancient and mystical forest, where sunlight filtered through emerald leaves,...



What If Vietnam Never Happened: Foresight and Hindsight in Graham Greene's The Quiet American

Published in 1955, Graham Greene's *The Quiet American* is considered a masterpiece of 20th-century literature. The story follows Thomas Fowler, a middle-aged British journalist,...