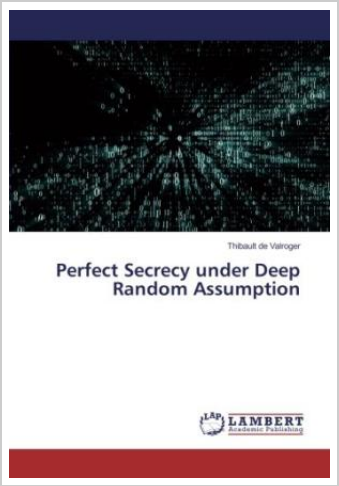

Perfect Secrecy under Deep Random Assumption

By Thibault de Valroger

LAP Lambert Academic Publishing Dez 2017, 2017. Taschenbuch. Condition: Neu. Neuware - Modern cryptography mostly relies on mathematical problems commonly trusted as very difficult to solve, such as large integer factorization or discrete logarithm, belonging to complexity theory. No certainty exist on the actual difficulty of those problems, not even the truth of the famous P NP conjecture. Furthermore, most of them are not resistant to quantum computing, which should make them useless in the next decades. In this work, a new idea is presented to design secure communication protocols capable to resist to unlimited opponents. Those protocols use a new form of randomness, called ' Deep Random ', capable to hide its probability distribution to the observers, and thus to prevent them performing Bayesian inference over public information to estimate the private information. The theoretical foundations are established, and an example is presented with its proof of security. 88 pp. Englisch.

Reviews

Extremely helpful for all group of men and women. it absolutely was writtern extremely perfectly and valuable. Your way of life span will be transform when you complete looking at this ebook.

-- ***Prof. Trever Torphy***

This publication is definitely not effortless to get going on looking at but really exciting to read through. It really is rally intriguing throgh looking at time period. Its been written in an remarkably straightforward way which is just soon after i finished reading through this book where basically altered me, change the way i think.

-- ***Erna Langosh***