Complexity

Special Issue on
Complexity and Cryptography: Advances and Challenges

WILEY | Hindawi

CALL FOR PAPERS

A cryptographic system or cryptosystem is used to secure the confidential data. At the transmitter, a cryptographic algorithm is applied on the confidential data with a cryptographic key to transform it to an unreadable format. At receiver, it is restored to original form by applying the cryptographic key with the inverse cryptographic algorithm. Cryptography is the art and science of designing secure and efficient cryptosystems; cryptanalysis is a part that deals with the breaking of cryptosystems and cryptology encompasses both cryptography and cryptanalysis. Since ever, experts from cryptography and cryptanalysis are working in parallel, but in opposition.

With the sophistication of cryptography and proposals such as Advanced Encryption Standard, it becomes almost impossible to break the contemporary cryptosystems completely. Nevertheless, the codebreakers rely on the computational complexity of the cryptosystems to somewhat break them within the given computational resources. The goal is to significantly reduce the number of iterations to the extent where a brute force attack is practically possible. Thus, the security of modern cryptography partially relies upon the computational complexity instead of completely breaking the cryptosystems.

There is a strong relationship between theoretical computational complexity and theoretical cryptography. Both try to solve or break those problems which are almost impossible for the binary computers in a meaningful time. Furthermore, considering complexity in cryptography, it is required to guard every aspect and instance of cryptosystem against having the low or weak computational complexity. On the other hand, the approach of using the theoretical computational complexity in breaking the cryptosystem utilises algorithmic reductions, genetic algorithms, neural networks, and evolutionary game theory.

The goal followed in this special issue is to create a volume of recent works on advances and challenges in those aspects of cryptanalysis and cryptosystems that deal with the computational complexity of these cryptosystems.

Potential topics include but are not limited to the following:

- The computational complexity of cryptosystems
- Algebraic complexity
- Communication complexity
- Nonlinear aspects of cryptosystems
- Construction of substitution boxes and their theoretical complexity
- Cryptanalysis of chaos-based cryptosystems
- Linear and differential cryptanalysis
- Integral cryptanalysis attacks
- Impossible differential cryptanalysis

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/complexity/ccac/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Muhammad A. Gondal, Dhofar University, Salalah, Oman
mgondal@du.edu.om

Guest Editors
Iqtadar Hussain, Qatar University, Doha, Qatar
iqtadarqau@qu.edu.qa

Amir Anees, La Trobe University, Melbourne, Australia
a.anees@latrobe.edu.au

Submission Deadline
Friday, 7 December 2018

Publication Date
April 2019