University of Manitoba

Pacific Institute *for the* Mathematical Sciences

PIMS-UManitoba Distinguished Lecture

Joan Boyar

(University of Southern Denmark)

4:00pm
October 18, 2018

Robert B. Schultz Lecture Theatre
University of Manitoba

Multiplicative Complexity of Cryptographic Functions

A symmetric key cryptosystem is one in which the same secret key is used for both encryption and decryption. An encryption function in a block symmetric key cryptosystem is a function of both the key and a block of n bits of data, and the result would generally be n bits long. The bits can be considered to be values in GF(2), and these functions are called Boolean functions. Such an encryption function must be highly nonlinear, or the system can be broken.

One measure of the nonlinearity of a Boolean function is its multiplicative complexity, which is the number of modulo 2 multiplications (ANDs) needed to compute the function, if the only operations allowed are multiplication and addition of two values modulo 2 (AND and XOR) and adding 1 modulo 2 to a value (NOT). This talk will be a survey of some results concerning multiplicative complexity, including a comparison to some other measures of nonlinearity. Multiplicative complexity turns out to be interesting in another way in settings such as homomorphic encryption and multi-party cryptographic protocols, where it can be important that the functions being computed have low multiplicative complexity.

JOAN BOYAR is a Professor of Computer Science at the University of Southern Denmark and Head of their Algorithms Group. She has a Bachelor degree in Mathematics from the University of Chicago. Her Masters and PhD degrees in Computer Science are from the University of California - Berkeley. She was a member of the Danish Natural Sciences Research Council for four years.

Her research interests are in the broad area of algorithms and complexity, especially cryptology, online algorithms, and complexity theory. Some of the work she is best known for is related to multiplicative complexity.

For more details visit: https://www.pims.math.ca/scientific-event/181018-pdljb