Fast Software Encryption 2017

Shiho Moriai
NICT, Japan

Design, Analysis and Promotion of (Lightweight) Block Ciphers

Abstract: During my 20+ year career in cryptographic research, I was blessed with opportunity to design several cryptographic algorithms. Two successful examples are design of block ciphers Camellia and CLEFIA. For some researchers, after they design, analyze, and implement the cryptosystem, presentation of the paper at a conference may be the goal. However, it was not the end for me. I tackled with the standardization and promotion of the ciphers. In this talk I will talk about success, difficulties, and what I learned through the activities.