Are Lightweight Block Ciphers Good Enough to Secure Our Data?

Title of the dissertation: Studies in Lightweight Cryptography
Tutkimuksia kevyen luokan salaustekniikasta

Contents of the dissertation:
The growing prevalence of pervasive computing devices has created a significant demand for lightweight ciphers suitable with respect to both efficiency and security. Lack of secure lightweight cipher can lead to serious risks and devastating attacks in extensively used applications. In response to this challenge, several attempts have been made to develop well understood and analyzed cryptographic designs. In particular, several lightweight block ciphers with novel structures have been designed during the last years. It is of utmost importance to evaluate the security of the emerging lightweight block ciphers.
This dissertation consists of two parts. The first part studies the criteria which are important for constrained applications. This is followed by studying the choices that have been made in the process of designing lightweight block ciphers. The second part proposes a set of novel cryptanalytic methods to determine the exact security level of some of the most promising designs for lightweight cryptographic algorithms. The research work includes both mathematical and structural analysis of the cryptographic constructions. These methods are useful for finding the best lightweight cryptography constructions to satisfy the predefined requirements.

Field of the dissertation: Computer science, Cryptography

Doctoral candidate: Hadi Soleimany, M.Sc.
Born in Iran 1984

Time of the defence: 30.01.2015 time 12

Place of the defence: Aalto University School of Science, lecture hall T2, Konemiehentie 2, Espoo

Opponent: Professor Carlos Cid, Royal Holloway, University of London, United Kingdom
Professor Andrey Bogdanov, Technical University of Denmark, Denmark

Custos: Professor Kaisa Nyberg, Aalto University School of Science, Department of Information and Computer Science

https://aaltodoc.aalto.fi/handle/123456789/52

Doctoral candidate’s contact information:
Hadi Soleimany
Department of Information and Computer Science
hadi.soleimany@aalto.fi
+358-449951488