Jun Rao

INF 501

Dr. Igor Steinmacher

BLOCK CIPHERS FOCUS ON THE LINEAR LAYER

Research Topic Overview

Block ciphers in cryptosystems are one of the most prominently used cryptographic primitives, and the linear layer is a core component in any substitution-permutation network block cipher. The Advanced Encryption Standard (AES) is a significant step forward in the field of block cipher design. Not only does AES offer robust security, but its structure also inspired many cipher designs ever since. Dr.Tolga's research is focused on the methodology to construct functional, sometimes optimal, linear layers allowing for a large variety of trade-offs.

As it stands, there are two general ways for the design of linear layers. The first one is to design it in a somewhat ad-hoc fashion, without following the general layout. This method might result in very secure and efficient algorithms, but it is not very well-pleasing from a scientific point-of-view. Another general design strategy is the wide-trail strategy which the main idea is to link the number of active S-boxes for linear and differential cryptanalysis to the minimal distance of a particular linear code associated with the successive layer of the cipher. However, there are virtually no general constructions or guidelines that would allow a substitution-permutation network (SPN) design to benefit from security vs. efficiency trade-offs. In response to this, Dr.Tolga's research and presentation is centered on the linear layer construction, and top underlines its value by presenting a new block cipher. Using such an approach to uncover alternative methods

for 8-bit micro-controllers will significantly enhance the capabilities regarding code size and cycle count.

The application of linear layers is rooted in a simple and powerful applicability concept that a block-interleaving construction which allows combining several strong linear mappings on a few numbers of bits into a robust linear layer for a more significant amount of bits. An optimal trade-off between hardware-efficiency and the number of active S-boxes is the point in which the concept of the most efficient linear layer theory is being incorporated into the algorithm development outlined in Dr.Tolga's presentation. Dr. Afghah also explained that by designing a new block cipher named PRIDE that significantly outperforms all existing block ciphers of similar key-sizes. The key points here is that our construction of strong linear layers is nicely in line with a bit-sliced implementation of the S-box layer.

Research Connections

I was able to distinguish some critical connections between my INF638 class which is Cryptography and Cryptosystems and that of Dr.Tolga's research. Since a significant portion of my course is focused on the underlying motivation, definition, and application of cryptography and cryptosystems, understanding linear layer -based algorithms to determine a balance point between the security and efficiency could be of vital importance. More specifically, the evolution of the linear layer could essentially emulate applications of cryptosystem theory in that what is best for a single cryptograph method will likely be the best for all given a specific set (security and efficiency) of minimal sacrifices.