Block ciphers – past and present

Lars Ramkilde Knudsen

DTU Compute, Denmark
lrkn@dtu.dk

Abstract. In the 1980s researchers were trying to understand the design of the DES, and breaking it seemed impossible. Other block ciphers were proposed, and cryptanalysis of block ciphers got interesting. The area took off in the 1990s where it exploded with the appearance of differential and linear cryptanalysis and the many variants thereof which appeared in the time after. In the 2000s AES became a standard and it was constructed specifically to resist the general attacks and the area of (traditional) block cipher cryptanalysis seemed saturated.... Much of the progress in cryptanalysis of the AES since then has come from side-channel attacks and related-key attacks.

Still today, for most block cipher applications the AES is a good and popular choice. However, the AES is perhaps not particularly well suited for extremely constrained environments such as RFID tags. Therefore, one trend in block cipher design has been to come up with ultra-lightweight block ciphers with good security and hardware efficiency. I was involved in the design of the ciphers Present (from CHES 2007), PrintCipher (presented at CHES 2010) and PRINCE (from Asiacrypt 2012). Another trend in block cipher design has been try to increase the efficiency by making certain components part of the secret key, e.g., to be able to reduce the number of rounds of a cipher.

In this talk, I will review these results.