An Algebraic Approach to the Design of Block Ciphers

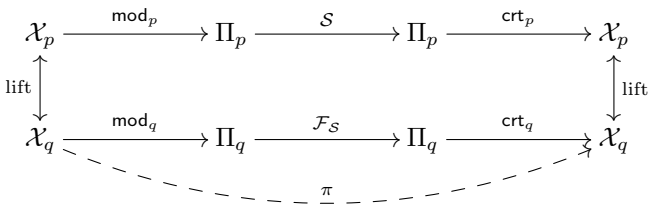
José Manuel E. Valença <jmvalenca at di.uminho.pt>*

Óscar Pereira <oscar at di.uminho.pt>*

We explore the possibility of modelling a working block cipher, and analysing its security, exclusively through an algebraic framework of polynomial rings and finite fields: one aims to get the simplest formal models of ciphers for which it is possible to get demonstrative evidence of its security but still with reasonably efficient implementations.

For this we propose a class of confusion-diffusion permutations (CDP's) grounded on two quotient polynomial rings $\mathcal{X}_q \equiv \mathbb{F}_2[z]/\langle q\rangle$, $\mathcal{X}_p \equiv \mathbb{F}_2[z]/\langle p\rangle$generated by two coprime, square-free monic polynomials with the same degree. The factorization of both q, p induce two product rings Π_q and Π_p which are ring isomorphic to $\mathcal{X}_q$ and $\mathcal{X}_p$ through the Chinese Remainder Theorem (CRT). The polynomial q is chosen in order to make multiplications efficient; the polynomial p is chosen such that it factorizes in irreducible distinct polynomials of odd degree. The ring Π_p is a product of fields which, unlike Π_q, allows "good" S-boxes to be constructed at the component level; e.g. almost bent boolean functions.

The following diagram represents the overall structure of a CDP $\pi\colon \mathcal{X}_q \to \mathcal{X}_q$. The permutations mod_p and mod_q are the inverse of crt_p and crt_q; lift is the identity map. The permutation $\mathcal{S}$ is a diagonal mapping of "good" permutation S-boxes; the permutation $\mathcal{F}_\mathcal{S}$ is implicitly defined in order to make the diagram commute.



With the permutation π, a round function is defined over $\mathcal{X}_q$ with two keys $\mu \in \mathcal{X}_q \setminus 0$ and $\upsilon \in \mathcal{X}_q^* \setminus 1$, as $\sigma\colon x \mapsto \pi(x + \mu) \times \upsilon$ and the resulting substitution permutation network is a simple sequential composition of these round functions. The diagram gives a two fold view of the permutation π and round function σ. For implementation purposes, the p-view is more relevant to π, whereas the q-view is more relevant to the round function (σ).

The immunity of this setup to linear, differential and algebraic attacks, as well as its diffusion properties, will be studied almost exclusively by looking at the properties of $\mathcal{F}_\mathcal{S}$. The main tool for this approach is harmonic analysis on finite fields.

*HASLab, Departamento de Informática, Universidade do Minho, 4710-057 Braga, Portugal