

S-Boxes and Filters

Hans Dobbertin, Magnus Daum, Patrick Felke, Tanja Lange, Gregor Leander

Horst Görtz Institute for IT-Security, University of Bochum

A *S(ubstitution)-box* is a mapping from $GF(2)^n$ to $GF(2)^m$ (a Boolean vector function), which is applied as a building block in a block cipher. The notion of a *filter* (Boolean function) is used when $m = 1$, a typical building block in a stream cipher. One of the classical topics of cryptography is the design of S-Boxes and filters, having certain attacks in mind.

The selection of criteria and the development of concrete construction realizing these criteria are sophisticated problems.

The selection is always risky, since there might occur weaknesses with respect to future attacks: A recent prominent example is AES. The byte-byte S-box of AES is defined, up to an affine modification, as $y = 1/x$ in the field $GF(2^8)$. Thus the quadratic equation $xy = 1$ holds, and therefore, given plain/cipher blocks, the reconstruction of the key can be reduced to solving a binary quadratic equational system, with very many unknowns unfortunately. This fact has recently caused much yet unresolved excitement, since it was argued that certain elimination techniques (linearization) could dramatically reduce the effort to compute the solution, i.e. the key.

The AES-box was selected as optimal with respect to their resistance against the differential and the linear attack, but not to avoid low degree input-output dependencies. It is a kind of ironic that, with respect to the latter, it is not only bad, actually it represents the worst case.

The construction of S-boxes and filters that fulfill cryptographic criteria is often difficult. For instance, the nonlinearity properties related to the differential and to the linear attack lead to lots of yet open problems.

On the other hand in about the last eight years there has been great progress in the study of nonlinear power functions, like the AES-box. Today we have a collection of mathematical theorems, which as we conjecture cover *all* optimal power function (at least for $n \leq 25$ this has been confirmed by computer experiments). However, the nonlinearity of power functions is still a great challenge for future research: Are there more optimal power functions than the ones we know? In case that n is even the actual optimal bound for the nonlinearity with respect to the linear attack is unknown (there is only a very reasonable conjecture). Are there “almost perfect nonlinear (APN) permutations if n is even? Especially, are there APN S-boxes for $n=8$)? (The AES-box is *not* APN.) Recall that APN is related to the differential attack.

Concerning filters we mention only one open basic problem. It is unknown for even $n \geq 8$: what is the optimal bound for the nonlinearity of a balanced filter? (For odd $n \geq 9$ this question is even completely hopeless.)

The construction of strong S-boxes and filters is not only based on mathematical insight, but experimental hill-climbing techniques - another important aspect of future research.

It is remarkable that many mathematical problems associated with the construction of cryptographically strong, highly nonlinear S-boxes and filters had been known in mathematics for a long time already. They had occurred in the study of codes, sequences and finite geometries.

We anticipate in future more new ideas to attack block ciphers, the mentioned algebraic approach will not be the last. Accordingly we shall then have to derive new criteria and constructions.