AES and the Wide Trail Design Strategy

Joan Daemen[1] and Vincent Rijmen[2,3]

[1] ProtonWorld, Zweefvliegtuigstraat 10, B-1130 Brussel, Belgium
Joan.Daemen@protonworld.com
[2] CRYPTOMAThIC, Lei 8A, B-3001 Leuven, Belgium
Vincent.Rijmen@cryptomathic.com
[3] IAIK, Graz University of Technology
Inffeldgasse 16a/1, A-8010 Graz, Austria

Rijndael is an iterated block cipher that supports key and block lengths of 128 to 256 bits in steps of 32 bits. It transforms a plaintext block into a ciphertext block by iteratively applying a single round function alternated by the addition (XOR) of a round keys. The round keys are derived from the cipher key by means of a key schedule. As a result of the wide trail strategy, the round function of Rijndael consists of three dedicated steps that each have a particular role. Rijndael versions with a block length of 128 bits, and key lengths of 128, 192 and 256 bits have been adopted as the Advanced Encryption Standard (AES).

The main cryptographic criterion in the design of Rijndael has been its resistance against differential and linear cryptanalysis. Differential cryptanalysis exploits differential trails ("characteristics") with high probability, Linear cryptanalysis exploits linear trails ("linear approximation") with high correlations ("bias"). Differential and linear trails have in common that they are both structures that propagate over multiple rounds. We show that in key-alternating ciphers such as Rijndael, their probability/correlation is independent of the value of the key. This greatly simplifies the estimation of the resistance against linear and differential cryptanalysis.

The structure of the Rijndael round function imposes strict upper limits to the correlation and probability of multiple-round trails. By combining diffusion operations based on MDS codes with byte transpositions in the round function, we obtain a provable lower bound of 25 active S-boxes in any four-round trail.

Linear trails and differential trails may combine to give rise to correlation and difference propagation probability values that are significantly higher than those of individual trails. We show the effect of the combination of trails for the case of a fixed key for any iterated block cipher and averaged over all round keys for key-alternating ciphers.

The most powerful attacks against Rijndael are saturation attacks. These attacks exploit the byte-oriented structure of the cipher and can break round-reduced variants of Rijndael up to 6 (128-bit key and state) or 7 rounds.

Rijndael can be completely specified with operations in GF(2^8). How the elements of GF(2^8) are represented in bytes can be seen as a detail of the specification, important for interoperability only. We can make abstraction from the representation of the elements of GF(2^8) and consider a block cipher that operates on strings of elements of GF(2^8). We call this generalization Rijndael-GF.

Rijndael is an instance of Rijndael-GF, where the representation of the elements has been specified.

Intuitively, it seems obvious that if Rijndael has a cryptographic weakness, this is inherited by Rijndael-GF and any instance of it. Traditionally, linear and differential cryptanalysis are done at the bit level and hence require to choose one specific representation of GF(2^8). We demonstrate how to conduct differential and linear propagation analysis at the level of elements of GF(2^8), without having to deal with representation issues.