Practical-Titled Attack on AES-128 Using Chosen-Text Relations

Vincent Rijmen

Introduction

Related-key attacks on AES-192 and AES-256 have been presented at Crypto 2009 and Asiacrypt 2009. Although these results are already quite spectacular, they have been extended to *practical-complexity* attacks on AES variants with 10 rounds at Eurocrypt 2010.

These advances in cryptanalysis are enabled by the introduction of a new type of related keys. Let the secret key be denoted by k, the round keys by k_i and describe the action of the key schedule of an arbitrary AES variant by: $k_i = \psi_i(k),\ i = 1, 2 \ldots$ The AES-256 adversary specifies two *key-differences-in-the-middle* ϵ, δ and queries the AES-256 implementation using the following related keys:

$$k^{(a,b)} = \psi^{-3.5}(\psi^{2.5}(\psi(k) + a\delta) + b\epsilon),\ a, b \in \{0, 1\}.$$

Chosen-text relations

Borrowing the powerful concept of chosen-key-relations-in-the-middle, I present here a new attack on AES-128. Note that strengthening AES-128 by adopting the AES-256 key schedule would *not* increase the resistance against the attack.

The attack: Let $R_k(x)$ denote the round transformation of AES. Furthermore, let δ denote any 16-byte string and define $\epsilon = \text{ShiftRows}^{-1}\left(\text{MixColumns}^{-1}(\delta)\right)$. Let $\{p, p^*\}$ denote the pair of plaintexts chosen by the adversary, where p is selected arbitrarily and p^* is uniquely defined by:

$$p^* = {R_k}^{-1}\left(R_k(p) + \delta\right).$$

It can easily be verified that k is a solution of

$$\text{SubBytes}(p + k) + \text{SubBytes}(p^* + k) = \epsilon.$$

If all bytes of ϵ are nonzero, then this equation has at most 2^{32} solutions. All solutions can be enumerated in a few seconds on a standard PC.

Observe that this adversary *doesn't* need to see the ciphertexts. The entropy of the key is reduced from 128 to 32 bits without making a single query to the encryption oracle. As far as I know, this is the first *zero-query attack* on a symmetric encryption primitive.

Conclusions

This attack clearly endangers all practical applications where an attacker can halt the computer in the middle of the execution of an encryption routine, apply the specific difference δ to the state, and roll back the interrupted encryption and obtain the modified plaintext p^*.

A similar attack can be mounted on KASUMI.