Doctored Dobbertin v2

The following text is generated by ChatGPT

This question mainly assesses the participants' mastery of tweakable block cipher analysis methods and their ability to read academic papers.

Description

The question describes the implementation of a 10-round tweakable AES algorithm, where the encryption function takes an additional input called the tweak, in addition to the plaintext and the key.

The server randomly generates a key, plaintext, and tweak, and then performs one encryption as a challenge. Subsequently, the client can choose plaintext and tweak to obtain the encryption result with the same key. Then, the server reveals the challenge ciphertext and the tweak used. The client needs to recover the plaintext to obtain the flag.

Solution

Upon comparison, it is evident that, in contrast to the original "Doctored Dobbertin" challenge from hack.lu CTF 2023, this question modifies constants including S-boxes, P-boxes, and constants, while reducing the number of chosen plaintext attacks from 7 to 1. Conventional methods like linear and differential cryptanalysis typically require more data. Therefore, alternative specialized methods should be considered.

If you search for "tweakable block cipher backdoor," you will find the related paper, and the attack method used in this question is derived from Section 5. Of course, solving this question does not necessarily require reading the original paper. Experienced participants may notice that the modification of round constants in the question seems suspicious: in each round of encryption, a constant and the tweak are added to the internal state separately. Is there a tweak that, when added to the derived round tweak for each round, cancels out the round constant? The answer is yes. Through analysis, it can be found that this tweak value is `0x846a51a2787d09d057b2bfa8a3481dae`. Then, we only need to send plaintext consisting of all zeros. Just before the last round key addition, we know that the first and third columns of the internal ciphertext must be equal, and the second and fourth columns must be equal. As half of the round keys in the last round are zeros, we can extract 8 non-zero key bytes. From there, we can determine 8 bytes of the master key, and

then we only need to enumerate the remaining 2 bytes of the master key.