Report for Presentation

Jing Yang

Tuesday 9th March, 2021

1 Summary

A stream cipher takes a key K and a public initial vector IV as the input and outputs a random-like sequence, usually called *keystream*. Each keystream bit can be regarded as a boolean function of K and IV. Usually, the first keystream bit is considered, and here we denote it as $f(\boldsymbol{k}, \boldsymbol{v})$, with $\boldsymbol{k}, \boldsymbol{v}$ denoting K and IV, respectively. It is interesting to recover $f(\boldsymbol{k}, \boldsymbol{v})$ or to explore any weakness of it to further find possible attacks. However, for a well-designed cipher, $f(\boldsymbol{k}, \boldsymbol{v})$ is very complex with a high degree and many monomials, and it is impossible to recover it or even store it. Instead, people turn to recover the *superpoly* of $f(\boldsymbol{k}, \boldsymbol{v})$ given an input *cube*, and by find a good cube, it is possible to give a distinguishing attack (showing that the cipher is not purely random) or key recovery attack. This is referred to as a cube attack.

A *cube* is the set of all possible values of a chosen subset of IV bits, with other non-chosen IV bits set to be constant (either 0 or 1). Thus the *superpoly* is defined as the sum of $f(\boldsymbol{k}, \boldsymbol{v})$ over all values of the cube. This superpoly could be much simplified compared to the original $f(\boldsymbol{k}, \boldsymbol{v})$ if a good cube is chosen and thus some secret key bits are possibly recovered.

Tradition cube attacks are experimental attacks by regarding the cipher as a blackbox, and the size of the cube is restricted to e.g., 40. In Eurocrypt 2015, Todo introduced a term called *division property*, which gives information about the xor-sum value of the output given an input multiset (e.g., a cube), i.e., *whether the xor-sum is zero or unknown*. This property can be propagated according to different rules for common basic operations in a cipher, e.g., `XOR, COPY, AND` (other complex operations like `Sbox, Modular Addition` can be regarded as combinations of these basic operations). The propagation can be modeled as a MILP problem, and be solved very efficiently using an optimization tool such as Gurobi. Thus by evaluating the propagation of the division property, it is expected to recover a superpoly much more efficiently.

This paper gives a stronger and more efficient cube attack, by utilizing division property based on *three subsets*: i.e., the xor-sum of the output given an input multiset is either *0, 1* or *unknown*, which is more accurate. It proposes a new MILP model for the propagation of the division property, and a very easy technique to verify if a specific monomial is involved into the superpoly by solving the MILP model. By this improved method, they refute some results from previous work and provide some more powerful attacks.

2 Importance of the Work

The paper proposes a more accurate and efficient method to explore a cube attack. It refutes some results from previous work and also provides more powerful attacks to some ciphers. Besides, their attack is much more efficient and easy to implement. This is of significance not only to a cryptanalyst, but also to the designers.

3 Improvements

Obviously, the contribution of the paper is of importance for both designers and cryptanalysts. The paper is well-written, provides detailed background knowledge to step in. But I would prefer to see more explanation about the new proposed techniques, describing why they can work and what does it mean in the cube attack.

For this direction, it seems that people are seeking to explore more accurate and efficient attacks, while the links to other relevant attacks are not extensively investigated, which is interesting and can be explored.