More Efficient Reconstruction of RC4 Keys from the Internal State

Mete Akgün
Pınar Kavak
Hüseyin Demirci
TUBİTAK-UEKAE

Previous Results on KSA of RC4

- In 1995 A. Roos observed relation between the key bytes and the initial terms of the state table
- At SAC 2007 Paul and Maitra have shown the probability model of this bias and given an algorithm to derive the key from the initial table. They used the bias of S[i] of initial elements.
- At FSE 2008 Biham and Carmeli improved these results by considering the differences of the entries to obtain information about the key:

  S[i1] – S[i2]

Our Work

- Under the same assumptionf of Biham and Carmeli consider the difference of j-th terms:i.e.
- $j_{i1} - j_{i2}$ in addition to S[İ1] – S[İ2]
- The bias coming from the terms is independent of the first one!
- For instance, the bias is more significant in the final parts of the table.

Results

- Combining the biases makes the key derivation much more powerful. For instance:
- For 40 bits of RC4, we reach a success rate of 96% at 0.025 seconds. The previous record was about 87% at the same time.
- For 128 bits of RC4, we obtain a success rate of 0.02 in a few minutes, compared with the previos rate:0.0005.

Thanks for your listening