Some Results on Sprout - DTU Orbit (08/11/2017)

Some Results on Sprout

Sprout is a lightweight stream cipher proposed by Armknecht and Mikhalev at FSE 2015. It has a Grain-like structure with two state Registers of size 40 bits each, which is exactly half the state size of Grain v1. In spite of this, the cipher does not appear to lose in security against generic Time-Memory-Data Tradeoff attacks due to the novelty of its design. In this paper, we first present improved results on Key Recovery with partial knowledge of the internal state. We show that if 50 of the 80 bits of the internal state are guessed then the remaining bits along with the secret key can be found in a reasonable time using a SAT solver. Thereafter, we show that it is possible to perform a distinguishing attack on the full Sprout stream cipher in the multiple IV setting using around 240 randomly chosen IVs on an average. The attack requires around 248 bits of memory. Thereafter, we will show that for every secret key, there exist around 230 IVs for which the LFSR used in Sprout enters the all zero state during the keystream generating phase. Using this observation, we will first show that it is possible to enumerate Key-IV pairs that produce keystream bits with period as small as 80. We will then outline a simple key recovery attack that takes time equivalent to 266.7 encryptions with negligible memory requirement. This although is not the best attack reported against this cipher in termncryptions with negligible memory requirement. This although is not the best attack reported against this cipher in terms of the time complexity, it is the best in terms of the memory required to perform the attack.

General information

State: Published
Organisations: Cryptology, Department of Applied Mathematics and Computer Science
Authors: Banik, S. (Intern)
Pages: 124-139
Publication date: 2015

Host publication information

Title of host publication: Progress in Cryptology – INDOCRYPT 2015 : Proceedings of the 16th International Conference on Cryptology in India
Publisher: Springer
Editors: Biryukov, A., Goyal, V.
ISBN (Print): 978-3-319-26616-9
ISBN (Electronic): 978-3-319-26617-6

Series: Lecture Notes in Computer Science
Volume: 9462
ISSN: 0302-9743
BFI conference series: INDOCRYPT (5010749)
Main Research Area: Technical/natural sciences
Conference: 16th International Conference on Cryptology in India, Bangalore, India, 06/12/2015 - 06/12/2015
Grain v1, Sprout, Stream cipher
DOIs:
10.1007/978-3-319-26617-6_7
Source: FindIt
Source-ID: 2290354217
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015