Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013 - DTU Orbit (08/11/2017)

Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013

For any modern chip design with a considerably large portion of logic, design for test (DFT) is a mandatory part of the design process which helps to reduce the complexity of testing sequential circuits. Scan-chains are one of the most commonly-used DFT techniques. However, the presence of scan-chains makes the device vulnerable to scan-based attacks from a cryptographic point of view. Techniques to cryptanalyze stream ciphers like Trivium, with additional hardware for scan-chains, are already available in literature (Agrawal et al. Indocrypt 2008). Such ideas were extended to more complicated stream ciphers like MICKEY 2.0 in the paper by Banik et al. at Indocrypt 2013. In this paper, we will look at the Double-Feedback XOR-Chain based countermeasure that was proposed by Banik et al. in Indocrypt 2013, to protect scan-chains from such scan-based attacks. We will show that such an XOR-Chain based countermeasure is vulnerable to attack. As an alternative, we propose a novel countermeasure based on randomization of XOR gates, that can protect scan-chains against such attacks.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science , Cryptology, Nanyang Technological University, Indian Institute of Technology
Authors: Banik, S. (Intern), Chattopadhyay, A. (Ekstern), Chowdhury, A. (Ekstern)
Pages: 179-196
Publication date: 2014

Host publication information

Title of host publication: Proceedings of the 15th International Conference on Cryptology in India (INDOCRYPT 2014)
Publisher: Springer
ISBN (Print): 978-3-319-13038-5
ISBN (Electronic): 978-3-319-13039-2

Series: Lecture Notes in Computer Science
Volume: 8885
ISSN: 0302-9743
BFI conference series: INDOCRYPT (5010749)
Main Research Area: Technical/natural sciences
Conference: 15th International Conference on Cryptology in India, New Delhi, India, 14/12/2014 - 14/12/2014
Scan-based attack, MICKEY 2.0, Double-Feedback XORChain scheme
DOIs:

10.1007/978-3-319-13039-2_11
Source: FindIt
Source-ID: 2287902773
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015