Findings Annihilator(s) via Fault Injection Analysis (FIA) on Boolean Function of LILI-128

ABSTRACT

LILI-128 keystream generator was designed by Dawson et al. (2000) and it was submitted to NESSIE project. This LILI-128 algorithm is a LFSR based synchronous stream cipher come with 128 bit key length. LILI-128 was designed to implement in hardware and software based and its offer large period and linear complexity. In this algorithm, the Boolean function given with coefficients, n is equal to ten (10) and its degree, d is equal to six (6). In conducting this attack, we aim to decrease the degree of the targeted Booleanequation by find it vulnerability with constructing low degree annihilator equation(s). We adopt the Fault Injection Analysis (FIA) methodology to achieve our objectives. In this study, we found the vulnerability via annihilator(s) through FIA (inject with value of one (1)) on Boolean function of LILI-128. With these injected Boolean functions, we proceed to utilize Hao's method to find new annihilator(s). Then we obtained new annihilator(s) on Boolean function of LILI-128 stream cipher. As a result, these newly identified annihilators successfully reduce the complexity of the published Boolean function to guess the initial secret key. It likewise gives truly necessary data on the security of these chose stream cipher concerning Fault Injection Analysis.

Keyword: Vulnerabilities; Annihilator; Boolean function; Fault Injection Analysis (FIA); Stream cipher; Algebraic attack