Abstract

Based on the Cube Attack by Itai Dinur and Adi Shamir and another, in the essence similar, method we devised a new polynomial linearisation technique, which proved to be more powerful, than the Cube Attack alone. Moreover, we present detailed description with formal proof not only of our findings, but also of the Cube Attack. Finally, we demonstrate the results of our efforts on a Trivium variant that is reduced in key and initialisation vector bit count. We managed to linearise polynomials representing a keystream bit output after up to 621 initialisation rounds using purely techniques described in this thesis, compared to 581 initialisation rounds with original attack.